デベロッパーガイド

AWS Config

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Config: デベロッパーガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

AWS Configとは 1
考慮事項 1
の使用方法 AWS Config 1
リソースの管理 1
監査とコンプライアンス 2
設定変更の管理とトラブルシューティング 2
セキュリティ分析 2
パートナーソリューション 3
機能 3
AWS Config の仕組み 4
リソース検出 5
リソーストラッキング 5
設定項目の配信 6
へのアクセスを制御する AWS Config 9
用語と概念 9
AWS Config インターフェイス 10
リソース管理 11
構成レコーダー 11
配信チャネル 6
AWS Config ルール 13
コンフォーマンスパック 17
アグリゲータ 17
AWS サービス統合 18
AWS Organizations 18
AWS Control Tower 19
AWS CloudTrail 19
AWS Security Hub 19
AWS Trusted Advisor 20
AWS Audit Manager 20
AWS Systems Manager 21
AWS Firewall Manager 21
Amazon EC2 専有ホスト 21
アプリケーション ロード バランサー 22
AWS CodeBuild 22

AWS X-Ray ... 22
AWS Service Management Connector ... 22
Amazon API Gateway ... 23
リージョンのサポート ... 23
考慮事項 ... 23
サポートされているリージョンのリスト ... 24
サービスの制限 ... 28
補足情報 ... 31
AWS のソフトウェア開発キット AWS Config ... 32
開始方法 ... 34
にサインアップする AWS ... 34
にサインアップする AWS アカウント ... 34
管理アクセスを持つユーザーを作成する ... 35
の使用を開始する方法 AWS Config ... 36
のセットアップ (コンソール) ... 36
設定 ... 36
ワンクリックセットアップ ... 37
手動セットアップ ... 40
設定 (AWS CLI) ... 47
設定 ... 47
前提条件 ... 48
開始 AWS Config ... 116
セットアップの確認 ... 119
AWS SDKs の使用 ... 121
構成レコーダー ... 123
カスタマーマネージド設定レコーダーに関する考慮事項 ... 123
サービスにリンクされた設定レコーダーに関する考慮事項 ... 125
サポートされる サービス ... 125
設定レコーダーのドリフト検出 ... 126
カスタマーマネージド設定レコーダーの起動 ... 127
カスタマーマネージド設定レコーダーの停止 ... 127
カスタマーマネージド設定レコーダーの記録頻度の変更 ... 128
カスタマーマネージド設定レコーダーの名前変更 ... 131
設定レコーダーの表示 ... 132
設定レコーダーの削除 ... 133
配信チャネル ... 135

考慮事項 135
用語 136
設定項目のコンポーネント 137
配信チャネルの表示 138
配信チャネルの更新 140
配信チャネルの名前変更 144
設定スナップショットを配信する 146
設定スナップショットを配信する 146
配信ステータスを確認する 146
設定スナップショットの表示 147
設定スナップショットの表示 148
設定スナップショットの例 148
通知の例 153
設定項目の変更の通知例 154
設定履歴の配信通知の例 170
設定スナップショットの配信開始の通知例 170
設定スナップショットの配信通知の例 171
コンプライアンス変更の通知の例 172
ルールの評価開始の通知例 176
サイズが大きすぎる設定項目の変更の通知例 177
配信失敗の通知の例 180
AWS Config ダッシュボード 182
コンプライアンスおよびリソースインベントリ 182
AWS Config 使用状況と成功のメトリクス 184
リソース管理 187
サポートされているリソースタイプ 188
Amazon AppStream 189
Amazon AppFlow 189
..... 190
Amazon API Gateway 190
Amazon Athena 191
Amazon Bedrock 191
Amazon CloudFront 191
Amazon CloudWatch 192
Amazon CodeGuru 193
Amazon Cognito 193

Amazon Connect 194
Amazon Detective 195
Amazon DynamoDB 195
Amazon EC2 195
Amazon ECR 204
Amazon ECS 205
Amazon EFS 206
Amazon EKS 206
Amazon EMR 207
Amazon EventBridge 207
Amazon Forecast 208
Amazon Fraud Detector 208
Amazon GuardDuty 209
Amazon Inspector 210
Amazon IVS 210
Amazon Keyspaces 210
Amazon OpenSearch Service 211
Amazon Personalize 212
Amazon Pinpoint 212
Amazon QLDB 213
Amazon Kendra 213
Amazon Kinesis 214
Amazon Lex 214
Amazon Lightsail 215
Amazon Lookout for Metrics 215
Amazon Lookout for Vision 216
Amazon Macie 216
Amazon Managed Grafana 216
Amazon Managed Service for Prometheus 216
Amazon MemoryDB 217
Amazon MQ 217
Amazon MSK 217
Amazon QuickSight 218
Amazon Redshift 218
Amazon RDS 220
Amazon Route 53 221

Amazon SageMaker AI 223
Amazon SES 225
Amazon SNS 225
Amazon SQS 225
Amazon S3 226
Amazon WorkSpaces 228
AWS Amplify 228
AWS AppConfig 228
AWS App Runner 229
AWS App Mesh 230
AWS AppSync 230
AWS Audit Manager 231
AWS Auto Scaling 231
AWS Backup 232
AWS Batch 233
AWS Billing and Cost Management 233
AWS Budgets 234
AWS Certificate Manager 234
AWS CloudFormation 234
AWS CloudTrail 235
AWS Cloud9 235
AWS Cloud Map 235
AWS CodeArtifact 236
AWS CodeBuild 236
AWS CodeDeploy 237
AWS CodePipeline 237
AWS Config 238
AWS DMS 239
AWS DataSync 239
AWS Device Farm 241
AWS Elastic Beanstalk 241
AWS Entity Resolution 242
AWS FIS 242
AWS Global Accelerator 243
AWS Glue 243
AWS Ground Station 244

AWS HealthLake 244
AWS IAM 244
AWS IoT 246
AWS KMS 249
AWS Lambda 250
AWS Mainframe Modernization 250
AWS Network Firewall 250
AWS Network Manager 251
AWS Panorama 252
AWS Private CA 253
AWS Resilience Hub 253
AWS Resource Explorer 254
AWS RoboMaker 254
AWS Signer 254
AWS Secrets Manager 255
AWS Security Hub 255
AWS Service Catalog 255
AWS Shield 256
AWS Step Functions 257
AWS Systems Manager 257
AWS Transfer Family 258
AWS WAF 258
AWS X-Ray 260
エラスティックロードバランシング 260
MediaConnect 261
MediaPackage 262
MediaTailor 263
利用可能なリージョン別リソースカバレッジ 263
北米および南米 263
欧州 323
アジアパシフィック 368
中国 465
アフリカおよび中東 485
GovCloud 511
AWS リソースの記録 535
考慮事項 536

リージョンリソースとグローバルリソース 536
AWS Config ルールとグローバルリソースタイプ 540
記録頻度 541
記録されていないリソース 542
リソースの記録 (コンソール) 543
リソースの記録 (AWS CLI) 547
リソースの除外 554
記録の停止 555
サードパーティリソースの記録 (AWS CLI) 555
リソースの追加 556
設定項目の記録 560
設定項目の読み取り 561
リソースの削除 562
ソフトウェア設定の記録 562
前提条件 563
ソフトウェア設定の記録 564
リソースの検索 565
リソースの表示 567
コンプライアンスの表示 (コンソール) 568
コンプライアンス (AWS SDKsの表示 568
コンプライアンス履歴の表示 576
コンプライアンス履歴の表示 (コンソール) 576
コンプライアンス履歴の表示 (AWS CLI) 577
リソースとルールの場合 583
コンプライアンス履歴のクエリ 584
リソースのタグ付け 585
タグ付けに関連する制限 585
AWS Config API アクションによるタグの管理 586
AWS Config ルール 587
考慮事項 587
リージョンのサポート 590
ルールのコンポーネント 598
AWS Config ルールの仕組み 599
トリガータイプ 600
評価モード 601
ルールのメタデータ 602

マネージドルール 603
マネージドルールのリスト 604
評価モード別のマネージドルールのリスト 1119
トリガータイプ別のマネージドルールのリスト 1142
リージョンアベイラビリティー別のマネージドルールのリスト 1164
AWS CloudFormation テンプレートを使用した マネージドルールの作成 1719
カスタムルール 1721
カスタムポリシールール 1721
カスタム Lambda ルール 1721
AWS Config カスタムルールの形式の違い 1722
カスタムポリシールールの作成 1722
カスタム Lambda ルールの作成 1729
カスタム Lambda ルールにより削除されたリソースを管理する 1751
サービスにリンクされたルール 1753
組織ルール 1754
考慮事項 1754
デプロイ 1755
リージョンのサポート 1756
ルールの追加 1760
コンソールを使用する 1760
AWS SDKsの使用 1763
ルールの更新 1766
コンソールを使用する 1767
AWS SDKsの使用 1767
ルールの削除 1771
考慮事項 1771
コンソールを使用する 1772
AWS SDKsの使用 1772
ルールの表示 1774
コンソールを使用する 1774
AWS SDKsの使用 1775
プロアクティブな評価を有効にする 1787
コンソールを使用する 1787
AWS SDKsの使用 1790
評価を Security Hub に送信する 1794
ルール評価を Security Hub に送信する 1794

ルールでのリソースの評価 1795
評価結果の削除 1799
トラブルシューティング 1800
コンフォーマンスパック 1803
適合パックのダッシュボード 1804
コンフォーマンスパックのメインページへの移動 1804
前提条件 1805
ステップ 1: AWS Config 録画を開始する 1805
ステップ 2: コンフォーマンスパックタイプ別の追加の前提条件 1805
リージョンのサポート 1811
プロセスチェック 1818
サンプルテンプレート 1819
プロセスチェックの作成 1820
コンプライアンスステータスの変更 1820
表示と編集 1822
コンフォーマンスパックのサンプルテンプレート 1822
AWS Control Tower Detective ガードレールコンフォーマンスパック 1826
ABS CCIG 2.0 マテリアルワークロードに関する運用上のベストプラクティス 1827
ABS CCIG 2.0 標準ワークロードに関する運用上のベストプラクティス 2054
ACSC の Essential 8 に関する運用上のベストプラクティス 2217
ACSC の「ISM」に関する運用上のベストプラクティス 2242
AI と機械学習に関する運用面のベストプラクティス 2378
Amazon API Gateway 運用のベストプラクティス 2378
Amazon CloudWatch に関する運用上のベストプラクティス 2379
Amazon DynamoDB に関する運用上のベストプラクティス 2379
Amazon S3 に関する運用上のベストプラクティス 2379
APRA の「CPG 234」に関する運用上のベストプラクティス 2379
アセット管理に関する運用上のベストプラクティス 2610
の運用のベストプラクティス AWS Backup 2611
AWS Identity and Access Management に関する運用上のベストプラクティス 2611
AWS Well-Architected フレームワークの信頼性の柱に関する運用上のベストプラクティス 2611
AWS Well-Architected フレームワークのセキュリティの柱に関する運用上のベストプラクティス 2678
BCP と DR に関する運用上のベストプラクティス 2842
BNM の「RMiT」に関する運用上のベストプラクティス 2843

カナダサイバーセキュリティセンター (CCCS) 中規模クラウド制御プロファイルに関する運用面のベストプラクティス 3158
CIS AWS Foundations Benchmark v1.4 Level 1 に関する運用上のベストプラクティス ... 4671
CIS AWS Foundations Benchmark v1.4 Level 2 の運用上のベストプラクティス 4715
CIS の「Critical Security Controls v8 IG1」に関する運用上のベストプラクティス 4773
CIS の「Critical Security Controls v8 IG2」に関する運用上のベストプラクティス 4872
CIS の「Critical Security Controls v8 IG3」に関する運用上のベストプラクティス 5047
CIS の「Top 20」に関する運用上のベストプラクティス 5236
CISA サイバーエッセンシャル 運用のベストプラクティス 5316
Criminal Justice Information Services (CJIS) の運用のベストプラクティス 5520
CMMC 2.0 Level 1 に関する運用上のベストプラクティス 5651
CMMC 2.0 Level 2 に関する運用上のベストプラクティス 5774
コンピューティングサービスに関する運用上のベストプラクティス 6183
データの回復性に関する運用上のベストプラクティス 6184
データベースサービスに関する運用上のベストプラクティス 6184
データレイクと分析サービスに関する運用上のベストプラクティス 6184
DevOP s 運用のベストプラクティス 6185
EC2 に関する運用上のベストプラクティス 6185
暗号化とキー管理に関する運用上のベストプラクティス 6185
SME 向け ENISA サイバーセキュリティガイドの運用上のベストプラクティス 6185
「Esquema Nacional de Seguridad (ENS) Low」に関する運用のベストプラクティス 6346
「Esquema Nacional de Seguridad (ENS) Medium」に関する運用のベストプラクティス 6454
「Esquema Nacional de Seguridad (ENS) High」に関する運用のベストプラクティス 6578
FDA Title 21 CFR Part 11 の運用のベストプラクティス 6709
FedRAMP (Low) の運用のベストプラクティス 7008
FedRAMP(Moderate) に関する運用上のベストプラクティス 7278
FedRAMP (High Part 1) の運用のベストプラクティス 7824
FedRAMP (High Part 2) の運用のベストプラクティス 8408
FFIEC に関する運用上のベストプラクティス 8537
ドイツのクラウドコンピューティングコンプライアンス条件カタログ (C5) の運用上のベストプラクティス 8761
グラムリーチブライリー法 (GLBA) に関する運用上のベストプラクティス 8849
GxP EU Annex 11 に関する運用上のベストプラクティス 8896
HIPAA Security の運用のベストプラクティス 9063
IRS 1075 に関する運用上のベストプラクティス 9540
K-ISMS の運用のベストプラクティス 9756

ロードバランシングの運用のベストプラクティス 9842
ログ記録に関する運用上のベストプラクティス 9843
サービスの管理およびガバナンスの運用のベストプラクティス 9843
シンガポール金融管理局の「Notice 655」の運用のベストプラクティス 9843
MAS TRMGの運用のベストプラクティス 9885
モニタリングの運用のベストプラクティス 10110
NBC の「TRMG」の運用のベストプラクティス 10111
NERC CIP BCSI に関する運用上のベストプラクティス 10548
NCSC Cloud Security Principles に関する運用上のベストプラクティス 10597
NCSC の「Cyber Assesment Framework」に関する運用上のベストプラクティス 10707
ネットワークおよびコンテンツ配信サービスの運用のベストプラクティス 10895
NIST の「800-53 rev 4」の運用のベストプラクティス 10895
NIST の「800-53 rev 5」の運用のベストプラクティス 11224
NIST 800 171 に関する運用上のベストプラクティス 11872
NIST の「800 172」の運用のベストプラクティス 12220
NIST の「800 181」の運用のベストプラクティス 12298
NIST の「1800 25」に関する運用上のベストプラクティス 12813
NIST の「CSF」に関する運用上のベストプラクティス 12984
NIST プライバシーフレームワーク v1.0 オペレーションのベストプラクティス 13360
NYDFS 23 の運用のベストプラクティス 13620
NZISM 3.8 の運用上のベストプラクティス 13800
PCI DSS 3.2.1 運用のベストプラクティス 13951
PCI DSS 4.0 の運用上のベストプラクティス (グローバルリソースタイプを除く) 14268
PCI DSS 4.0 の運用上のベストプラクティス (グローバルリソースタイプを含む) 14603
パブリックにアクセス可能なリソースの運用のベストプラクティス 15023
RBI の「Cyber Security Framework for UCBs」に関する運用上のベストプラクティス ... 15023
RBI の「MD-ITF」の運用のベストプラクティス 15073
セキュリティ、ID、コンプライアンスの運用のベストプラクティス 15227
サーバーレスの運用のベストプラクティス 15227
ストレージサービスの運用のベストプラクティス 15227
SWIFT CSP の運用のベストプラクティス 15227
Amazon Elastic Container Service (Amazon ECS) のセキュリティのベストプラクティス 15262
Amazon Elastic File System (Amazon EFS) のセキュリティのベストプラクティス 15263
Amazon Elastic Kubernetes Service (Amazon EKS) でのセキュリティに関するベストプラクティス 15263
Amazon CloudFront のセキュリティのベストプラクティス 15263

Amazon OpenSearch Service のセキュリティベストプラクティス 15264
Amazon Redshift のセキュリティベストプラクティス 15264
Amazon Relational Database Service (Amazon RDS) でのセキュリティに関するベストプラクティス 15264
AWS Auto Scalingのセキュリティのベストプラクティス 15264
AWS CloudTrailのセキュリティのベストプラクティス 15265
AWS CodeBuildのセキュリティのベストプラクティス 15265
Amazon ECR のセキュリティのベストプラクティス 15265
AWS Lambdaのセキュリティのベストプラクティス 15266
AWS Network Firewallのセキュリティのベストプラクティス 15266
Amazon SageMaker AI のセキュリティのベストプラクティス 15266
AWS Secrets Managerのセキュリティのベストプラクティス 15266
AWS WAFのセキュリティのベストプラクティス 15267
修正アクションを含むテンプレートの例 15267
カスタムテンプレートの作成 15267
用語 15268
テンプレートのカスタマイズ 15268
適合パックのデプロイ 15273
適合パックの編集 15276
適合パックの削除 15277
考慮事項 15278
コンフォーマンスパックを削除するには 15278
適合パックの表示 15279
コンプライアンス履歴の表示 15282
コンプライアンスのタイムラインの表示 15283
コンプライアンス履歴のクエリ 15284
組織のコンフォーマンスパックの管理 15285
考慮事項 15286
デプロイ 15287
リージョンのサポート 15288
トラブルシューティング 15291
適合パックの失敗ステータス 15292
適合パック内のダングリングルール 15293
修正 15295
リージョンのサポート 15295
手動修復の設定 15299

自動修復の設定 15301
修復アクションの削除 15303
アグリゲータ 15305
ユースケース 15305
用語 15306
リージョンのサポート 15306
アグリゲータダッシュボード 15311
アグリゲータダッシュボードの使用 15311
コンプライアンスダッシュボード 15314
インベントリダッシュボード 15316
アグリゲータの作成 15318
委任管理者の登録 15324
アグリゲータの編集 15326
アグリゲータの削除 15328
アグリゲータアカウントの承認 15328
考慮事項 15329
認証の追加 15329
認証の削除 15331
考慮事項 15331
認証の削除 15331
アグリゲータの表示 15332
トラブルシューティング 15333
高度なクエリ 15336
機能 15337
クエリコンポーネント 15337
概要 15337
パラメータ 15338
例 15338
クエリエディタ (コンソール) 15339
考慮事項 15339
AWS サンプルクエリを使用する 15339
カスタムクエリの作成 15340
クエリエディタ (AWS CLI) 15341
考慮事項 15341
リソース設定データのクエリ 15342
クエリの保存 15344

保存されたクエリをすべて表示 15344
保存されたクエリの詳細の取得 15345
保存されたクエリの削除 15345
自然言語クエリプロセッサ 15346
考慮事項 15346
自然言語クエリプロセッサを使用したクエリ 15339
プロンプトの例 15347
フィードバックの提供 15351
リージョンのサポート 15351
クエリ例 15352
関係のクエリの例 15358
制限 15360
CIDR 表記/IP 範囲 15361
配列内の複数のプロパティ 15362
リージョンのサポート 15363
データの削除 15368
データ保持期間の設定 (コンソール) 15370
セキュリティ 15372
データ保護 15373
転送時のデータの暗号化 15374
転送時のデータの暗号化 15374
Identity and Access Management 15374
対象者 15375
アイデンティティを使用した認証 15375
ポリシーを使用したアクセスの管理 15379
が IAM と AWS Config 連携する方法 15382
アイデンティティベースのポリシーの例 15388
AWS マネージドポリシー 15407
IAM ロールのアクセス許可 15576
IAM ロールの更新 15580
Amazon S3 バケットのアクセス許可 15582
KMS キーのアクセス許可 15586
Amazon SNS トピックへの許可 15589
トラブルシューティング 15593
サービスリンクロールの使用 15595
インシデントへの対応 15597

コンプライアンス検証 15597
耐障害性 15599
インフラストラクチャセキュリティ 15599
設定と脆弱性の分析 15599
サービス間の混乱した代理の防止 15600
ベストプラクティス 15600
ログ記録とモニタリング 15602
ログ記録 15602
AWS Config CloudTrail の情報 15602
AWS Config ログファイルエントリについて 15603
ログファイルの例 15604
モニタリング 15611
Amazon SQS の使用 15612
Amazon EventBridge の使用 15614
Amazon VPC エンドポイント 15621
VPC エンドポイントの作成 15621
よくある質問 15622
最新の設定変更が表示されない 15622
設定変更をすぐに表示することは可能ですか？ 15622
の間接的な関係 AWS Config 15622
リソース関係とは何ですか? 15622
リソースに関する直接的な関係と間接的な関係とは何ですか? 15623
はどの間接的な関係 AWS Config をサポートしていますか？ 15623
間接的な関係を使用するシナリオはどれですか？ 15625
直接的な関係と間接的な関係によって設定項目はどのように作成されますか? 15627
間接的な関係によって生成される設定項目にはどのようなものがありますか? 15627
間接的な関係を無効にするにはどうすればよいですか？ 15629
間接的な関係に関連する設定データを取得する方法を教えてください。 15629
コードの例 15630
基本 15630
アクション 15631
ドキュメント履歴 15668
以前の更新 15813
..... 15885

AWS Configとは

AWS Config は、アカウント AWS 内の AWS リソースの設定の詳細ビューを提供します。これには、リソース間の関係と設定の履歴が含まれるため、時間の経過と共に設定と関係がどのように変わるかを確認できます。

An AWS resource は、Amazon Elastic Compute Cloud (EC2) インスタンス AWS、Amazon Elastic Block Store (EBS) ボリューム、セキュリティグループ、Amazon Virtual Private Cloud (VPC) など、で操作できるエンティティです。でサポートされている AWS リソースの完全なリストについては AWS Config、「」を参照してください[でサポートされているリソースタイプ AWS Config](#)。

考慮事項

- AWS アカウント: アクティブな が必要です AWS アカウント。詳細については、「[AWSへのサインアップ](#)」を参照してください。
- Amazon S3 バケット: 設定スナップショットと履歴のデータを受信するには、S3 バケットが必要です。詳細については、[Amazon S3 バケットのアクセス許可](#)を参照してください。
- Amazon SNS トピック: 設定スナップショットと履歴に変更があった場合に通知を受け取るには、Amazon SNS が必要です。詳細については、「[Permissions for the Amazon SNS Topic](#)」を参照してください。
- IAM ロール: AWS Configにアクセスするのに必要なアクセス許可を持つ IAM ロールが必要です。詳細については、「[Permissions for the IAM Role](#)」を参照してください。
- リソースタイプ: 記録 AWS Config するリソースタイプを決定できます。詳細については、[AWS「リソースの記録](#)」を参照してください。

の使用方法 AWS Config

でアプリケーションを実行する場合 AWS、通常は AWS リソースを使用します。リソースはまとめて作成および管理する必要があります。アプリケーションの需要が増大するにつれて、 は AWS リソースを追跡する必要があります。 AWS Config は、以下のシナリオでアプリケーションリソースを監督するのに役立つように設計されています。

リソースの管理

リソースの設定に対するガバナンスを強化し、リソースの誤設定を検出するには、どのようなリソースがあり、どのように設定されているかを常に正確に把握しておく必要があります。 AWS Config を

使用して、各リソースに対して行われた呼び出しをポーリングすることで、これらの変更をモニタリングすることなく、リソースが作成、変更、または削除されるたびに通知を受け取ることができます。

AWS Config ルールを使用して、 リソースの設定を評価できます AWS 。がリソースがいずれかのルールの条件に違反していること AWS Config を検出すると、 はリソースを非準拠として AWS Config フラグ付けし、通知を送信します。 AWS Config は、リソースが作成、変更、または削除されるたびにリソースを継続的に評価します。

監査とコンプライアンス

使用しているデータが自社のポリシーやベストプラクティスに準拠していることを確認するために頻繁な監査を必要とする場合があります。コンプライアンスを確認するには、リソースの設定履歴にアクセスする必要があります。この情報は によって提供されます AWS Config。

設定変更の管理とトラブルシューティング

相互に依存する複数の AWS リソースを使用すると、1 つのリソースの設定が変更されると、関連リソースに意図しない結果が生じる可能性があります。を使用すると AWS Config、変更するリソースが他のリソースとどのように関連しているかを表示し、変更の影響を評価できます。

また、 AWS Config が提供するリソースの設定履歴を使用して、問題のトラブルシューティングを行ない、問題が発生したリソースの最後の正常であると判明している設定にアクセスできます。

セキュリティ分析

潜在的なセキュリティの弱点を分析するには、ユーザーに付与される AWS Identity and Access Management (IAM) アクセス許可や、 AWS リソースへのアクセスを制御する Amazon EC2 セキュリティグループルールなど、リソース設定に関する詳細な履歴情報が必要です。

を使用して AWS Config 、 が AWS Config 記録していたユーザー、グループ、またはロールに割り当てられた IAM ポリシーをいつでも表示できます。この情報に基づいて、特定の時間にユーザーに属していたアクセス許可を確認できます。例えば、ユーザー `John Doe` が 2015 年 1 月 1 日に Amazon VPC 設定を変更するアクセス許可を持っていたかどうかを表示できます。

AWS Config を使用して、特定の時間に開かれたポートルールなど、EC2 セキュリティグループの設定を表示することもできます。この情報により、特定のポートに着信する TCP トラフィックをセキュリティグループがブロックしていたかどうかを判断できます。

パートナーソリューション

AWS は、ログ記録と分析のサードパーティースペシャリストと提携し、 AWS Config 出力を使用するソリューションを提供します。詳細については、 AWS Config の詳細ページを参照してくださいAWS Config。

機能

をセットアップすると AWS Config、以下を完了できます。

リソース管理

- 記録 AWS Config するリソースタイプを指定します。

- 設定スナップショット (リクエストした場合) と設定履歴を受け取るように Amazon S3 バケットを設定する。
- 設定のストリーミング通知を送信するように Amazon SNS を設定する。
- Amazon S3 バケットと Amazon SNS トピックにアクセスするために必要なアクセス AWS Config 許可を付与します。

  詳細については、AWS 「リソース設定と履歴の表示」およびAWS 「リソース設定と履歴の管理」を参照してください。

ルールおよびコンフォーマンスパック

- 記録されたリソースタイプのコンプライアンス情報を評価するために AWS Config 使用するルールを指定します。
- 適合パック、 AWS アカウントで単一のエンティティとしてデプロイおよびモニタリングできるルールの集合。

  詳細については、AWS Config 「ルールとコンフォーマンスパックを使用したリソースの評価https://docs.aws.amazon.com/config/latest/developerguide/conformance-packs.html」を参照してください。

修正

- によって評価される非準拠のリソースを修正します AWS Config ルール。

詳細については、「Remediation」を参照してください。

アグリゲーター

- アグリゲーターを使用すると、リソースのインベントリとコンプライアンスを一元的に把握できます。アグリゲータは、複数の および AWS リージョンから AWS Config 設定 AWS アカウント とコンプライアンスのデータを 1 つのアカウントとリージョンに収集します。

  詳細については、[マルチアカウントマルチリージョンのデータ集約] を参照してください。

高度なクエリ

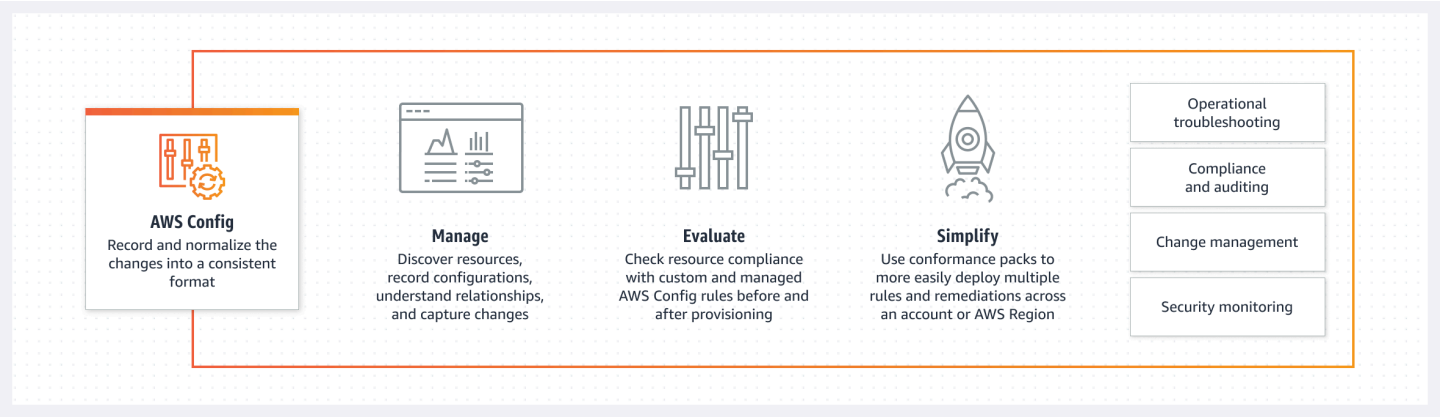
- サンプルクエリのいずれかを使用するか、 AWS リソースの設定スキーマを参照して独自のクエリを作成します。

  詳細については、AWS 「リソースの現在の設定状態のクエリ」を参照してください。

AWS Config の仕組み

AWS Config は、アカウント AWS 内の AWS リソースの設定の詳細ビューを提供します。これには、リソース間の関係と設定の履歴が含まれるため、時間の経過と共に設定と関係がどのように変わるかを確認できます。

An AWS resource は、Amazon Elastic Compute Cloud (EC2) インスタンス AWS、Amazon Elastic Block Store (EBS) ボリューム、セキュリティグループ、Amazon Virtual Private Cloud (VPC) など、で操作できるエンティティです。でサポートされている AWS リソースの完全なリストについては AWS Config、「」を参照してください[でサポートされているリソースタイプ AWS Config](#)。



リソース検出

有効にすると AWS Config、まずアカウントに存在するサポートされている AWS リソースを検出し、リソースごとに設定項目を生成します。

AWS Config は、リソースの設定が変更されると設定項目も生成し、設定レコーダーを起動したときのリソースの設定項目の履歴レコードを保持します。デフォルトでは、 はリージョンでサポートされているすべてのリソースの設定項目 AWS Config を作成します。サポートされているすべてのリソースの設定項目 AWS Config を作成しない場合は、追跡するリソースタイプを指定できます。

が追跡 AWS Config するリソースタイプを指定する前に、Resource Coverage by Region Availability をチェックして、リソースタイプがセットアップする AWS リージョンでサポートされているかどうかを確認します AWS Config。リソースタイプが少なくとも 1 つのリージョン AWS Config で でサポートされている場合は、指定したリソースタイプがセットアップしているリージョンをサポートしていない場合でも AWS Config、 でサポートされているすべての AWS リージョンでそのリソースタイプの記録を有効にできます AWS Config。

リソーストラッキング

AWS Config は、アカウント内の各リソースの Describe API コールまたは List API コールを呼び出すことで、リソースに対するすべての変更を追跡します。このサービスでは、その同じ API コールを使用して、すべての関連リソースの設定詳細をキャプチャします。

たとえば、VPC セキュリティグループから Egress ルールを削除する AWS Config と、 はセキュリティグループで Describe API コールを呼び出します。 AWS Config その後、 はセキュリティグループに関連付けられたすべてのインスタンスで Describe API コールを呼び出します。セキュリティグループ (リソース) と各インスタンス (関連リソース) の更新された設定が設定項目として記録され、設定のストリーミングで Amazon Simple Storage Service (Amazon S3) バケットに配信されます。

AWS Config は、API によって開始されなかった設定変更も追跡します。 AWS Config は、リソース設定を定期的に調べ、変更された設定の設定項目を生成します。

AWS Config ルールを使用している場合、 は必要な設定について AWS リソース設定 AWS Config を継続的に評価します。ルールに応じて、 AWS Config は設定の変更に応じて、または定期的にリソースを評価します。各ルールは、ルールの評価ロジックが含まれている AWS Lambda 関数に関連付けられます。がリソース AWS Config を評価すると、ルールの AWS Lambda 関数が呼び出されます。この関数は、評価されたリソースのコンプライアンスステータスを返します。リソースがルールの条件に違反した場合、 はリソースとルールを非準拠として AWS Config フラグ付けします。リソース

のコンプライアンスステータスが変更されると、 は Amazon SNS トピックに通知 AWS Config を送信します。

設定項目の配信

AWS Config は、次のいずれかのチャネルを介して設定項目を配信できます。

Amazon S3 バケット

AWS Config は AWS リソースの設定の変更を追跡し、指定した Amazon S3 バケットに更新された設定の詳細を定期的に送信します。が AWS Config 記録するリソースタイプごとに、6 時間ごとに設定履歴ファイルを送信します。各設定履歴ファイルには、その 6 時間の間に変更があったリソースの詳細が含まれています。各ファイルに含まれるリソースタイプは 1 つです (Amazon EC2 インスタンスや Amazon EBS ボリュームなど)。設定変更が行われない場合、 AWS Config はファイルを送信しません。

AWS Config は、CLI で deliver-config-snapshot コマンドを使用する場合、または AWS Config API AWS で DeliverConfigSnapshot アクションを使用する場合、設定スナップショットを Amazon S3 バケットに送信します。設定スナップショットには、 AWS アカウントで AWS Config が記録したすべてのリソースの設定詳細が含まれています。設定履歴ファイルと設定スナップショットは JSON 形式です。

> **Note**
>
> AWS Config は、設定履歴ファイルと設定スナップショットを指定された S3 バケットにのみ配信します。S3 バケット内のオブジェクトのライフサイクルポリシーは変更 AWS Config しません。ライフサイクルポリシーを使用して、オブジェクトを削除するか、Amazon S3 Glacier にアーカイブするかを指定できます。詳細については、Amazon Simple Storage Service Console ユーザーガイド中のライフサイクル設定の管理を参照してください。ブログ投稿の Amazon S3 データを S3 Glacier にアーカイブするも参照してください。

Amazon SNS トピック

Amazon Simple Notification Service (Amazon SNS) トピックは、E メールアドレスなどのサブスクライブしているエンドポイントやクライアントにメッセージ (または通知) を配信するために Amazon SNS で使用する通信チャネルです。その他の種類の Amazon SNS 通知として、携帯電話のアプリへのプッシュ通知メッセージ、SMS 対応の携帯電話やスマートフォンへのショートメッセージサービ

ス (SMS) 通知、HTTP POST リクエストなどがあります。最適な結果を得るために、SNS トピックの通知エンドポイントとして Amazon SQS を使用し、通知内の情報をプログラムで処理します。

AWS Config は、指定した Amazon SNS トピックを使用して通知を送信します。受信する通知の種類は、次の例に示すように、メッセージ本文の `messageType` キーの値で示されます。

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

通知のメッセージタイプは、以下のいずれかです。

メッセージタイプ	説明
ComplianceChangeNotification	が AWS Config 評価するリソースのコンプライアンスタイプが変更されました。コンプライアンスタイプは、リソースが特定の AWS Config ルールに準拠しているかどうかを示し、メッセージ内の `ComplianceType` キーで表されます。メッセージには、比較のために `newEvaluationResult` オブジェクトと `oldEvaluationResult` オブジェクトが含まれます。
ConfigRulesEvaluationStarted	AWS Config は、指定されたリソースに対するルールの評価を開始しました。
ConfigurationSnapshotDeliveryStarted	AWS Config は、Amazon S3 バケットへの設定スナップショットの配信を開始しました。Amazon S3 バケットの名前は、メッセージの `s3Bucket` キーで示されます。
ConfigurationSnapshotDeliveryCompleted	AWS Config は、設定スナップショットを Amazon S3 バケットに正常に配信しました。
ConfigurationSnapshotDeliveryFailed	AWS Config は、設定スナップショットを Amazon S3 バケットに配信できませんでした。
ConfigurationHistoryDeliveryCompleted	AWS Config は、設定履歴を Amazon S3 バケットに正常に配信しました。

メッセージタイプ	説明
ConfigurationItemChangeNotification	リソースが作成または削除されるか、設定が変更されました。このメッセージには、この変更に対して が AWS Config 作成する設定項目の詳細と、変更のタイプが含まれます。これらの通知は、変更後数分以内に配信され、まとめて設定ストリームと呼ばれます。
OversizedConfigurationItemChangeNotification	このメッセージタイプは、設定項目の変更通知が Amazon SNS の最大許容サイズを超えた時に配信されます。メッセージには設定項目の概要が含まれます。SMS メッセージを除き、Amazon SNS メッセージには、XML、JSON、フォーマットされていないテキストなど、最大 256 KB のテキストデータを含めることができます。完全な通知の参照先は、指定した Amazon S3 バケット内にあります。
OversizedConfigurationItemChangeDeliveryFailed	AWS Config は、オーバーサイズの設定項目の変更通知を Amazon S3 バケットに配信できませんでした。

通知の例については、「Amazon SNS トピック AWS Config に送信する通知」を参照してください。Amazon SNS の詳細については、Amazon Simple Notification Service デベロッパーガイド を参照してください。

> **Note**
>
> 最新の設定変更が表示されないのはなぜですか？
> AWS Config 通常、 は、変更が検出された直後、または指定した頻度でリソースの設定変更を記録します。ただし、これはベストエフォートベースであり、場合によっては時間がかかることがあります。問題がしばらく経過しても解決しない場合は、 サポートに連絡して、Amazon CloudWatch でサポートされている AWS Config メトリクスを指定します。これらの使用状況メトリクスの詳細については、「AWS Config Usage and Success Metrics」を参照してください 。

へのアクセスを制御する AWS Config

AWS Identity and Access Management は、Amazon Web Services (AWS) のお客様がユーザーとユーザーのアクセス許可を管理できるようにするウェブサービスです。

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- 以下のユーザーとグループ AWS IAM Identity Center：

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。
- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。
- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

AWS Config の用語と概念

このトピックでは AWS Config、理解しやすくするために、いくつかの主要な概念について説明します。

目次

- AWS Config インターフェイス
  - AWS Config コンソール
  - AWS Config CLI
  - AWS Config APIs
  - AWS Config SDKs
- リソース管理
  - AWS リソース
  - リソース関係

- 構成レコーダー
- 配信チャネル
  - 設定項目
  - 設定履歴
  - 設定スナップショット
  - 設定ストリーム
- AWS Config ルール
  - 評価結果
  - ルールタイプ
  - トリガータイプ
  - 評価モード
- コンフォーマンスパック
- マルチアカウントマルチリージョンのデータ集約
  - ソースアカウント
  - 送信元リージョン
  - アグリゲータ
  - サービスにリンクされたアグリゲータ
  - アグリゲータアカウント
  - Authorization

AWS Config インターフェイス

AWS Config コンソール

AWS Config コンソールを使用してサービスを管理できます。の詳細については AWS Management Console、「」を参照してくださいAWS Management Console。

AWS Config CLI

AWS Command Line Interface は、コマンドライン AWS Config から操作するために使用できる統合ツールです。詳細については、AWS Command Line Interface ユーザーガイドをご参照ください。CLI コマンドの完全なリストについては、 AWS Config 「使用可能なコマンド」を参照してください。

AWS Config APIs

コンソールと CLI に加えて、 AWS Config RESTful APIsを使用して AWS Config 直接プログラミングすることもできます。詳細については、「 APIリファレンスAWS Config」を参照してください。

AWS Config SDKs

AWS Config API を使用する代わりに、いずれかの AWS SDKsを使用できます。各 SDK は、各種のプログラミング言語とプラットフォームに対応したライブラリやサンプルコードで構成されています。SDK は、 AWS Configへのアクセス権をプログラムによって作成するのに役立ちます。例えば、SDK では、暗号を使用してリクエストに署名したり、エラーを管理したり、リクエストを自動的に再試行したりできます。詳細については、Amazon Web Services のツールページを参照してください。

リソース管理

の基本コンポーネントを理解すること AWS Config で、リソースのインベントリと変更を追跡し、AWS リソースの設定を評価するのに役立ちます。

AWS リソース

AWS リソースは、、 AWS Command Line Interface (CLI) AWS Management Console、 AWS SDKs。 AWS リソースの例としては AWS 、Amazon EC2 インスタンス、セキュリティグループ、Amazon VPCs、Amazon Elastic Block Store などがあります。 は、リソース ID や Amazon リソースネーム (ARN) などの一意の識別子を使用して各リソース AWS Config を参照します。が AWS Config サポートするリソースタイプのリストについては、「」を参照してくださいでサポートされているリソースタイプ AWS Config。

リソース関係

AWS Config はアカウント内の AWS リソースを検出し、 AWS リソース間の関係のマップを作成します。例えば関係には、セキュリティグループ `sg-ef678hk` に関連付けられている Amazon EC2 インスタンス `i-a1b2c3d4` に接続された Amazon EBS ボリューム `vol-123ab45d` が含まれる場合があります。

詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。

構成レコーダー

設定レコーダーは、範囲内のリソースタイプの設定変更を設定項目として保存します。詳細については、「設定レコーダーの使用」を参照してください。

設定レコーダーには 2 つのタイプがあります。

Type	説明
カスタマーマネージド設定レコーダー	管理した設定レコーダー。スコープ内のリソースタイプはユーザーが設定します。デフォルトでは、カスタマーマネージド設定レコーダー AWS Config は、 が実行されている AWS リージョン でサポートされているすべてのリソースを記録します。
サービスにリンクされた設定レコーダー	特定の にリンクされている設定レコーダー AWS のサービス。スコープ内のリソースタイプは、リンクされたサービスによって設定されます。

配信チャネル

は、 AWS リソースに発生した変更 AWS Config を継続的に記録し、配信チャネルを介して通知と更新された設定状態を送信します。配信チャネルを管理して、 が設定更新 AWS Config を送信する場所を制御できます。

設定項目

設定項目は、アカウントに存在するサポートされている AWS リソースのさまざまな属性のpoint-in-timeビューを表します。設定項目のコンポーネントには、メタデータ、属性、関係、現在の設定、関連イベントが含まれます。 は、記録するリソースタイプへの変更を検出するたびに設定項目 AWS Config を作成します。例えば、 AWS Config が Amazon S3 バケットを記録している場合、 はバケットが作成、更新、または削除されるたびに設定項目 AWS Config を作成します。 AWS Config でを選択して、設定した記録頻度で設定項目を作成することもできます。

詳細については、「Components of a Configuration Item」および「Recording Frequency」を参照してください。

設定履歴

設定履歴は、特定期間の特定リソースに関する設定項目のコレクションです。設定履歴から、リソースの最初の作成日、先月の設定内容、昨日午前 9 時に行われた設定変更などを確認できます。設定

履歴は複数の形式で利用できます。 は、記録されるリソースタイプごとに設定履歴ファイルを、指定した Amazon S3 バケット AWS Config に自動的に配信します。 AWS Config コンソールで特定のリソースを選択し、タイムラインを使用してそのリソースの以前のすべての設定項目に移動できます。また、リソースの設定項目の履歴には API からアクセスすることもできます。

詳細については、「Viewing Compliance History」と「Querying Compliance History」を参照してください。

設定スナップショット

設定スナップショットは、アカウント内のサポートされているリソースに関する設定項目のコレクションです。設定スナップショットは、記録対象のリソースとその設定の全体像を示します。設定スナップショットは設定を検証するのに役立ちます。例えば、設定スナップショットを定期的に調べて、設定が間違っているリソースや不要と思われるリソースを見つけることができます。設定スナップショットは複数の形式で利用できます。設定スナップショットは、ユーザーが指定した Amazon Simple Storage Service (Amazon S3) バケットに配信できます。さらに、 AWS Config コンソールでポイントインタイムを選択し、リソース間の関係を使用して設定項目のスナップショット内を移動できます。

詳細については、「Delivering Configuration Snapshots」、「Viewing Configuration Snapshots」、「Example Configuration Snapshot」を参照してください。

設定ストリーム

設定ストリームは、 が記録するリソースのすべての設定項目を自動的に更新したリスト AWS Config です。リソースが作成、変更、または削除されるたびに、 AWS Config は設定項目を作成して設定ストリームに追加します。設定のストリーミングでは、ユーザーが選択した Amazon Simple Notification Service (Amazon SNS) トピックを使用します。設定ストリームは、設定の変更が発生したときに監視して、潜在的な問題を検出したり、特定のリソースが変更された場合に通知を生成したり、 AWS リソースの設定を反映する必要がある外部システムを更新したりするために役立ちます。

AWS Config ルール

AWS Config ルールは、特定の AWS リソースの理想的な設定を管理するのに役立つコンプライアンスチェックです。 は、リソース設定が関連ルールに準拠しているかどうか AWS Config を評価し、コンプライアンス結果を表示します。

評価結果

AWS Config ルールには 4 つの評価結果があります。

評価結果	説明
COMPLIANT	ルールはコンプライアンスチェックの条件に合格します。
NON_COMPLIANT	ルールはコンプライアンスチェックの条件に失敗します。
ERROR	必須/オプションのパラメータの 1 つが無効であるか、正しいタイプではないか、形式が正しくありません。
NOT_APPLICABLE	ルールのロジックを適用できないリソースを除外するために使用されます。例えば、alb-desync-mode-check ルールは Application Load Balancer のみをチェックし、Network Load Balancer と Gateway Load Balancer は無視します。

ルールタイプ

ルールには 2 つのタイプがあります。ルール定義とルールメタデータの構造の詳細については、AWS Config 「 ルールのコンポーネント」を参照してください。

Type	説明	詳細情報
マネージドルール	によって作成された事前定義のカスタマイズ可能なルール AWS Config。	マネージドルールのリストについては、AWS Config 「 マネージドルールのリスト」を参照してください。
カスタムルール	ゼロから作成するルール。AWS Config カスタムルールを作成するには、Lambda 関数 (AWS Lambda デベロッパーガイド) と Guard (Guard	詳細については、「カスタムポリシールールの作成 AWS Config」およびAWS Config 「カスタム Lambda ルールの作成」を参照してください。

Type	説明	詳細情報
	GitHub リポジトリ) の 2 つの方法があります。	

トリガータイプ

アカウントにルールを追加すると、 はリソースをルールの条件 AWS Config と比較します。この最初の評価の後、 は評価がトリガーされるたびに評価の実行を AWS Config 続行します。評価のトリガーは、ルールの一部として定義されます。以下のタイプを含めることができます。

トリガータイプ	説明
設定変更	AWS Config は、ルールのスコープに一致するリソースがあり、リソースの設定が変更された場合に、ルールの評価を実行します。評価は、が設定項目の変更通知 AWS Config を送信した後に実行されます。 どのリソースで評価を開始するかは、ルールのスコープで定義します。スコープには以下を含めることができます。 • 1 つ以上のリソースタイプ • リソースタイプとリソース ID の組み合わせ • タグキーとタグ値の組み合わせ • 記録対象リソースの作成、更新、または削除時 AWS Config は、ルールのスコープに一致するリソースへの変更を検出すると、評価を実行します。スコープを使用して評価を開始するリソースを定義できます。
定期的	AWS Config は、24 時間ごとなど、選択した頻度でルールの評価を実行します。

トリガータイプ	説明
ハイブリッド	一部のルールでは、設定変更と定期的なトリガーの両方があります。これらのルールでは、は、設定の変更を検出したときと、指定した頻度でリソース AWS Config を評価します。

評価モード

AWS Config ルールには 2 つの評価モードがあります。

評価モード	説明
プロアクティブ	プロアクティブ評価は、デプロイ前のリソースを評価するために使用します。これにより、リージョンのアカウントにあるプロアクティブルールのセットを考慮して、 AWS リソースを定義するためにリソースプロパティのセットが COMPLIANT か NON_COMPLIANT かを評価することができます。 詳細については、「評価モード」を参照してください。プロアクティブ評価をサポートするマネージドルールのリストについては、「評価モード別の AWS Config マネージドルールのリスト」を参照してください。
検出	検出評価は、デプロイ済みのリソースを評価するために使用します。これにより、既存のリソース構成の設定を評価できます。

> **Note**
>
> プロアクティブルールは、NON_COMPLIANT のフラグが付けられたリソースを修正したり、これらのリソースのデプロイを妨げたりしません。

コンフォーマンスパック

コンフォーマンスパックは、アカウントとリージョンの単一のエンティティとして、または の組織全体に簡単にデプロイできる AWS Config ルールと修復アクションのコレクションです AWS Organizations。

コンフォーマンスパックは、 AWS Config マネージドルールまたはカスタムルールおよび修復アクションのリストを含む YAML テンプレートを作成することで作成します。テンプレートは、 AWS Config コンソールまたは AWS CLIを使用してデプロイできます。

すぐに開始して AWS 環境を評価するには、サンプルのコンフォーマンスパックテンプレートのいずれかを使用します。カスタムコンフォーマンスパックに基づいてコンフォーマンスパックの YAML ファイルをゼロから作成することもできます。カスタムコンフォーマンスパックは、 アカウントと AWS リージョン、または の組織全体に一緒にデプロイできる AWS Config ルールと修復アクションの一意のコレクションです AWS Organizations。

プロセスチェックは、コンフォーマンスパックの一部として検証が必要な外部タスクと内部タスクを追跡できる AWS Config ルールの一種です。これらのチェックは、既存のコンフォーマンスパックまたは新しいコンフォーマンスパックに追加できます。urations や手動チェックを含むすべてのコンプライアンスを 1 AWS Configか所で追跡できます。

マルチアカウントマルチリージョンのデータ集約

のマルチアカウントマルチリージョンデータ集約 AWS Config を使用すると、複数のアカウントとリージョンの設定データとコンプライアンスデータを 1 つのアカウントに集約 AWS Config できます。マルチアカウントマルチリージョンのデータ集約は、中央の IT 管理者がエンタープライズ AWS アカウント 内の複数の のコンプライアンスをモニタリングするのに役立ちます。アグリゲータを使用しても、追加コストは発生しません。

ソースアカウント

ソースアカウントは、 AWS Config リソース設定とコンプライアンスデータを集約する AWS アカウント です。ソースアカウントは、個別のアカウントまたは AWS Organizationsの組織を指定できます。ソースアカウントは個別に提供することも、取得することもできます AWS Organizations。

送信元リージョン

ソースリージョンは、 AWS Config 設定およびコンプライアンスデータを集約する AWS リージョンです。

アグリゲータ

アグリゲータは、複数のソースアカウントとリージョンから AWS Config 設定およびコンプライアンスデータを収集します。集約された AWS Config 設定とコンプライアンスデータを表示するリージョンにアグリゲータを作成します。

> **Note**
>
> アグリゲータでは、ソースアカウントからアグリゲータアカウントにデータをレプリケートすることにより、アグリゲータが閲覧を許可されているソースアカウントとリージョンに対して、読み取り専用ビューを提供します。アグリゲータでは、ソースアカウントまたはリージョンへの変更アクセスを提供しません。例えば、アグリゲータを使用してルールをデプロイしたり、アグリゲータを介してソースアカウントまたはリージョンにスナップショットファイルをプッシュしたりできないということを意味します。

サービスにリンクされたアグリゲータ

サービスにリンクされたアグリゲータは、特定の にリンクされます AWS のサービス。範囲内の設定データとコンプライアンスデータは、リンクされたサービスによって設定されます。

アグリゲータアカウント

アグリゲータアカウントは、アグリゲータを作成するアカウントです。

Authorization

ソースアカウントの所有者として、承認とは、 AWS Config 設定とコンプライアンスデータを収集するためにアグリゲータアカウントとリージョンに付与するアクセス許可を指します。 AWS Organizationsの一部であるソースアカウントを集約する場合、承認は必要ありません。

AWS とのサービス統合 AWS Config

AWS Config は、他のいくつかの AWS サービスとの統合をサポートしています。このリストは網羅的ではありません。

AWS Organizations

AWS Organizations を使用して、 AWS Configマルチアカウント、マルチリージョンのデータ集約機能に使用するアカウントを定義できます。 AWS Organizations は、複数の AWS アカウント を、作

成して一元管理する組織に統合するのに役立つアカウント管理サービスです。 AWS Organizations 詳細を指定することで、組織全体のコンプライアンスステータスをモニタリングできます。詳細については、「AWS Organizations ユーザーガイド」の「AWS Config および AWS Organizations」を参照してください。

AWS Control Tower

AWS Control Tower は、すべての登録済みアカウント AWS Config で を有効にするため、検出コントロールによるコンプライアンスのモニタリング、リソースの変更の記録、ログアーカイブアカウントへのリソース変更ログの配信を行うことができます。詳細については、「AWS Control Tower ユーザーガイド」の「Monitor resource changes with AWS Config」を参照してください。

AWS CloudTrail

AWS Config は と統合 AWS CloudTrail して、設定の変更をアカウント内の特定のイベントに関連付けます。CloudTrail ログを使用して、リクエストを行ったユーザー、時刻、IP アドレスなど、変更を呼び出したイベントの詳細を取得できます。CloudTrail コンソールから AWS Config タイムラインに移動して、 AWS API アクティビティに関連する設定変更を表示できます。

詳細については、「 AWS Config デベロッパーガイド」の「 を使用した AWS Config API コールのログ記録 AWS CloudTrail」および「 AWS CloudTrail ユーザーガイド」の「 コンソールを使用して AWS Config 設定項目用のイベントデータストアを作成する」を参照してください。

AWS Security Hub

AWS Security Hub は、 AWS Config ルールを含む他の AWS のサービスからセキュリティチェックを一元化します。Security Hub は、リソース設定がベストプラクティスに沿っていることを確認する AWS Config ルールを有効にして制御します。Security Hub が環境のリソースでセキュリティチェックを実行するすべてのリージョン AWS Config のすべてのアカウントで を有効にします。詳細については、「AWS Security Hub ユーザーガイド」の「AWS services that send findings to Security Hub」を参照してください。

> **Security Hub 関連のルールの中には、定期的なもので、設定項目に依存しないものがあります。**
>
> Security Hub 関連のルールの中には、定期的なものがあります。これらのルールは、設定レコーダーを有効にせずに実行でき、設定項目 (CI) に依存しません。

つまり、ルールページを表示すると、リストされている CI やサポートされているリソースはありません。リソース ID を選択すると、 というエラーが表示されますThe provided resource ID and resource type cannot be found。これは想定される動作です。

AWS Trusted Advisor

AWS Config マネージドルールは、すべてのカテゴリにわたって一連の Trusted Advisor チェックを強化します。特定のマネージドルールを有効にすると、対応する Trusted Advisor チェックが自動的に有効になります。特定の AWS Config マネージドルールによる Trusted Advisor チェックを確認するには、「 AWS サポート ユーザーガイド」のAWS Trusted Advisor 「 チェックリファレンス」を参照してください。

AWS Config パワードチェックは、AWS ビジネスサポート、AWS エンタープライズオンランプ、AWS エンタープライズサポートプランをご利用のお客様が利用できます。を有効に AWS Config し、これらの AWS サポートプランのいずれかがある場合、対応するデプロイされた AWS Config マネージドルールに基づく推奨事項が自動的に表示されます。

> **更新リクエストは許可されず、リソースは除外できません**
>
> これらのチェックの結果は、 AWS Config マネージドルールの変更によってトリガーされる更新に基づいて自動的に更新されます。更新要求は許可されません。現時点では、これらのチェックからリソースを除外することはできません。

詳細については、「 AWS サポート ユーザーガイド」の「 による Trusted Advisor チェックの表示 AWS Config」を参照してください。

AWS Audit Manager

Audit Manager を使用して、 AWS Config 評価を監査の証拠としてキャプチャできます。カスタムコントロールを作成または編集する場合、証拠収集のデータソースマッピングとして 1 つ以上の AWS Config ルールを指定できます。 はこれらのルールに基づいてコンプライアンスチェック AWS Config を実行し、Audit Manager は結果をコンプライアンスチェックの証拠として報告します。詳細については、「AWS Audit Manager ユーザーガイド」の「AWS Config Rules supported by AWS Audit Manager」を参照してください。

AWS Systems Manager

AWS Config は Systems Manager と統合して、オンプレミス環境の Amazon EC2 インスタンスとサーバーでソフトウェアの設定変更を記録します。この統合により、オペレーティングシステム (OS) 設定、システムレベルの更新、インストールされたアプリケーション、ネットワーク設定などに関する可視性を獲得できます。 AWS Config は、Amazon EC2 インスタンスに記録されたインフラストラクチャ設定変更とともに、OS およびシステムレベルの設定変更の履歴も提供します。Systems Manager コンソールから AWS Config タイムラインに移動して、マネージド Amazon EC2 インスタンスの設定変更を表示できます。を使用して AWS Config 、Systems Manager のインベントリ履歴を表示し、すべてのマネージドインスタンスの変更を追跡できます。

詳細については、「 AWS Systems Manager ユーザーガイド」の「 AWS サービスとの統合 | 管理とガバナンス、AWS Config 設定レコーダー、およびAWS Config コンフォーマンスパックのデプロイ」を参照してください。

AWS Firewall Manager

Firewall Manager を使用するには、 AWS Organizations メンバーアカウント AWS Config ごとに を有効にする必要があります。新しいアプリケーションが作成されると、Firewall Manager はファイアウォールルールを構築し、セキュリティポリシーを作成し、一貫して適用するための単一のサービスです。詳細については、「」の「 を有効にする AWS ConfigAWS WAF AWS Firewall Manager」、および「 AWS Shield Advanced デベロッパーガイド」を参照してください。

> **Note**
>
> Firewall Manager は継続的な記録に基づいてリソースのモニタリングを行います。Firewall Manager を使用している場合、記録頻度を連続に設定することをお勧めします。連続記録と毎日の記録の詳細については、「Recording Frequency」を参照してください。

Amazon EC2 専有ホスト

AWS Config は Amazon EC2 専有ホストと統合してライセンスコンプライアンスを評価します。 は専有ホストでインスタンスが起動、停止、またはシャットダウンされたときに AWS Config を記録し、この情報をホスト ID、Amazon マシンイメージ (AMI) IDs、ソケット数、物理コアなどのソフトウェアライセンスに関連するホストおよびインスタンスレベルの情報とペアにします。これにより、ライセンスレポートのデータソース AWS Config として を使用できます。Amazon EC2 Dedicated

Hosts コンソールから AWS Config タイムラインに移動して、Amazon EC2 Dedicated Hosts の設定変更を表示できます。

詳細については、「Linux インスタンス向け Amazon Elastic Compute Cloud ユーザーガイド」の「設定の変更を追跡する」または「Windows インスタンス向け Amazon Elastic Compute Cloud ユーザーガイド」の「設定の変更を追跡する」を参照してください。

アプリケーション ロード バランサー

AWS Config は Elastic Load Balancing (ELB) サービスと統合して、Application Load Balancer の設定変更を記録します。 には、関連する Amazon EC2 セキュリティグループ、VPCs、サブネットとの関係 AWS Config も含まれます。この情報は、セキュリティ分析とトラブルシューティングに役立ちます。例えば、どのセキュリティグループが Application Load Balancer に関連付けられているかを随時確認できます。ELB コンソールから AWS Config タイムラインに移動して、Application Load Balancer の設定変更を表示できます。

AWS CodeBuild

AWS Configは、 AWS リソースのインベントリと、これらのリソースの設定変更の履歴を提供します。 は AWS CodeBuild、 AWS リソースとして AWS Config をサポートします。つまり、サービスは CodeBuild プロジェクトを追跡できます。詳細については、「 AWS CodeBuild ユーザーガイド」のCodeBuild AWS Config での使用」サンプルを参照してください。

AWS X-Ray

AWS X-Ray は と統合 AWS Config して、X-Ray 暗号化リソースに加えられた設定変更を記録します。 AWS Config を使用して、X-Ray 暗号化リソースのインベントリ、X-Ray 設定履歴の監査、リソースの変更に基づく通知の送信を行うことができます。詳細については、「AWS X-Ray デベロッパーガイド」の「Tracking X-Ray encryption configuration changes with AWS Config」を参照してください。

AWS Service Management Connector

AWS Service Management Connector for ServiceNow は、アグリゲータを使用して複数のアカウントとリージョンの AWS Config データを同期できます。詳細については、「 AWS Service Management Connector 管理者ガイド」のServiceNow AWS Config での統合」を参照してください。

Amazon API Gateway

を使用して AWS Config 、API Gateway API リソースに加えられた設定変更を記録し、リソースの変更に基づいて通知を送信できます。API Gateway リソースの設定変更履歴を維持することは、運用上のトラブルシューティング、監査、およびコンプライアンスのユースケースに役立ちます。詳細については、「API Gateway デベロッパーガイド」の「AWS Configによる API Gateway API 設定のモニタリング」を参照してください。

のリージョンサポート AWS Config

考慮事項

の一部の機能は AWS Config 、 がサポートされている AWS リージョンのサブセットでのみサポート AWS Config されています。

リソース管理

- どの AWS リソースタイプがどのリージョンでサポートされているかのリストについては、「Resource Coverage by Region Availability」を参照してください。

AWS Config ルール

- どのリージョンでどの AWS Config ルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。
- AWS Config ルールの組織的なデプロイをサポートするリージョンのリストについては、「組織ルール | リージョンのサポート」を参照してください。

コンフォーマンスパック

- コンフォーマンスパックとコンフォーマンスパックの組織的なデプロイをサポートするリージョンのリストについては、「コンフォーマンスパック | リージョンのサポート」を参照してください。

修正

- AWS Config ルールの修復アクションをサポートするリージョンのリストについては、「修復アクション | リージョンのサポート」を参照してください。

アグリゲーター

- アグリゲータをサポートするリージョンのリストについては、「アグリゲータ | リージョンのサポート」を参照してください。

高度なクエリ

- 高度なクエリをサポートするリージョンのリストについては、「高度なクエリ | リージョンのサポート」を参照してください。
- 高度なクエリ用の自然言語クエリプロセッサをサポートするリージョンのリストについては、「Natural language query processor for advanced queries | Region Support」を参照してください。

サポートされているリージョンのリスト

次の表に、有効にできる AWS リージョンを示します AWS Config。

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
米国西部 (北カリフォルニア)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
アジアパシフィック (ハイデラバード)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
アジアパシフィック (マレーシア)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
アジアパシフィック (台北)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
アジアパシフィック (タイ)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
メキシコ (中部)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

のサービスの制限 AWS Config

次の表は、 内の制限を示しています AWS Config。特に明記されていない限り、クォータはリクエストに応じて引き上げることができます。クォータの引き上げをリクエストできます。

のその他の制限については AWS、AWS 「サービスの制限」を参照してください。

リソースタグ

説明	制限値	引き上げ可能
リソースあたりのタグの最大数	50	いいえ

AWS Config ルール

説明	制限値	引き上げ可能
アカウントあたりのリージョンあたりの AWS Config ルールの最大数	1,000	いいえ

単一アカウントのコンフォーマンスパック

説明	制限値	引き上げ可能
アカウントあたりのコンフォーマンスパックの最大数	50	いいえ
コンフォーマンスパックあたりの AWS Config ルールの最大数	130	いいえ

> **Note**
>
> AWS Config コンフォーマンスパックの ルールは、アカウントあたりのリージョンあたりの AWS Config ルールの最大数の制限に含まれます。

組織コンフォーマンスパック

説明	制限値	引き上げ可能
組織ごとのコンフォーマンスパックの最大数	50	いいえ
組織コンフォーマンスパックあたりの AWS Config ルールの最大数	130	いいえ

> **Note**
>
> 組織レベルでデプロイすると、子アカウントの 制限に がカウントされます。コンフォーマンスパックの AWS Config ルールは、アカウントあたりのリージョンあたりの AWS Config ルールの最大数 の制限に されます。

アグリゲータ

説明	制限値	引き上げ可能
設定アグリゲータの最大数	50	はい
アグリゲータ内のアカウントの最大数	10000	いいえ
すべてのアグリゲータで週ごとに追加または削除されるアカウントの最大数	1,000	はい

> **Note**
>
> 組織レベルのアグリゲータと個々のアカウントアグリゲータはどちらも、設定アグリゲータの最大数の制限にカウントされます。

高度なクエリ

説明	制限値	引き上げ可能
1 つのアカウントと 1 つのリージョンに保存されたクエリの最大数	300	はい

の補足情報および関連リソース AWS Config

このサービスを利用する際に役立つ関連リソースは次のとおりです。

- AWS Config - 情報のプライマリウェブページ AWS Config。
- AWS Config の料金
- テクニカル FAQ
- AWS Config Rule Development Kit (RDK) – さまざまな AWS リソースタイプを使用してルールを設定 AWS Config、作成、テストするのに役立つオープンソースツールです。
- パートナー – と完全に統合されたパートナー製品へのリンクです。 AWS Config これにより、設定ストリーム、設定スナップショット、または設定履歴からのデータを視覚化、モニタリング、管理できます。

- クラスとワークショップ – AWS スキルを磨き、実践的な経験を積むのに役立つセルフペースラボに加えて、ロールベースのコースと専門コースへのリンクです。
- AWS デベロッパーセンター – チュートリアルを詳しく調べたり、ツールをダウンロードしたり、デ AWS ベロッパーイベントについて学習したりできます。
- AWS デベロッパーツール – AWS アプリケーションを開発および管理するためのデベロッパーツール、SDKs、IDE ツールキット、コマンドラインツールへのリンク。
- 入門リソースセンター – のセットアップ方法 AWS アカウント、 AWS コミュニティへの参加方法、最初のアプリケーションを起動する方法について説明します。
- ハンズオンチュートリアル - ステップ バイ ステップのチュートリアルに従って、最初のアプリケーションを AWSで起動します。
- AWS ホワイトペーパー – ソリューションアーキテクトや他の技術エキスパートが AWS 作成したアーキテクチャ、セキュリティ、経済などのトピックを網羅した、技術 AWS ホワイトペーパーの包括的なリストへのリンクです。

- AWS サポート センター – AWS サポート ケースを作成および管理するためのハブ。フォーラム、技術上のFAQs、サービスヘルスステータス、 など、その他の役立つリソースへのリンクも含まれています AWS Trusted Advisor。
- サポート – クラウドでのアプリケーションの構築と実行に役立つ サポート one-on-one の迅速な対応のサポートチャネルである に関する情報のプライマリウェブページ。
- お問い合わせ - AWS の請求、アカウント、イベント、不正使用、その他の問題などに関するお問い合わせの受付窓口です。
- AWS サイト規約 – 当社の著作権と商標、お客様のアカウント、ライセンス、サイトアクセス、およびその他のトピックに関する詳細情報。

AWS のソフトウェア開発キット AWS Config

Software AWS Development Kit (SDK) を使用すると、費用対効果が高く、スケーラブルで信頼性の高い AWS インフラストラクチャサービスにアクセスするアプリケーションを簡単に構築できます。AWS SDK では、ライブラリ、コード例、参照資料がダウンロード可能な 1 つのパッケージにまとめられているため、数分で使用を開始できます。次の表に、 AWS Config プログラムで にアクセスするために使用できる SDKs とサードパーティーライブラリを示します。

アクセスのタイプ	説明
AWS SDKs	AWS には、次の SDKs。 • AWS SDK for C++ ドキュメント • AWS Mobile SDK for iOS ドキュメント • AWS SDK for Go のドキュメント • AWS SDK for Java ドキュメント • AWS SDK for JavaScript のドキュメント • AWS SDK for .NET ドキュメント • AWS SDK for PHP ドキュメント • AWS SDK for Python (Boto) ドキュメント • AWS SDK for Ruby ドキュメント
サードパーティライブラリ	デベロッパーコミュニティのデ AWS ベロッパーは、以下のデ AWS ベロッパーセンターにある独自のライブラリも提供します。

アクセスのタイプ	説明
	• AWS Java デベロッパーセンター • AWS JavaScript デベロッパーセンター • AWS PHP デベロッパーセンター • AWS Python デベロッパーセンター • AWS Ruby デベロッパーセンター • AWS Windows および .NET デベロッパーセンター

の開始方法 AWS Config

AWS Config は、 内の AWS リソースの設定の詳細ビューを提供します AWS アカウント。を使用すると AWS Config、 AWS リソース間の設定や関係の変更を確認し、リソース設定履歴を調べ、ルールを使用してコンプライアンスを判断できます。詳細については、「 AWS Configとは」およびAWS Config 「 の仕組み」を参照してください。

にサインアップする AWS

トピック

- にサインアップする AWS アカウント
- 管理アクセスを持つユーザーを作成する

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 を保護し AWS IAM Identity Center、 を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの AWS アカウント 「ルートユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、AWS IAM Identity Center 「 ユーザーガイド」の「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン 「 ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」を参照してください。

の使用を開始する方法 AWS Config

にサインアップしたら AWS アカウント、 AWS Management Console、 AWS CLI、または AWS SDKs AWS Config を使用して の使用を開始できます。

- コンソール AWS Config でのセットアップ
- AWS Config を使用した のセットアップ AWS CLI
- AWS SDK での AWS Config サービスの使用

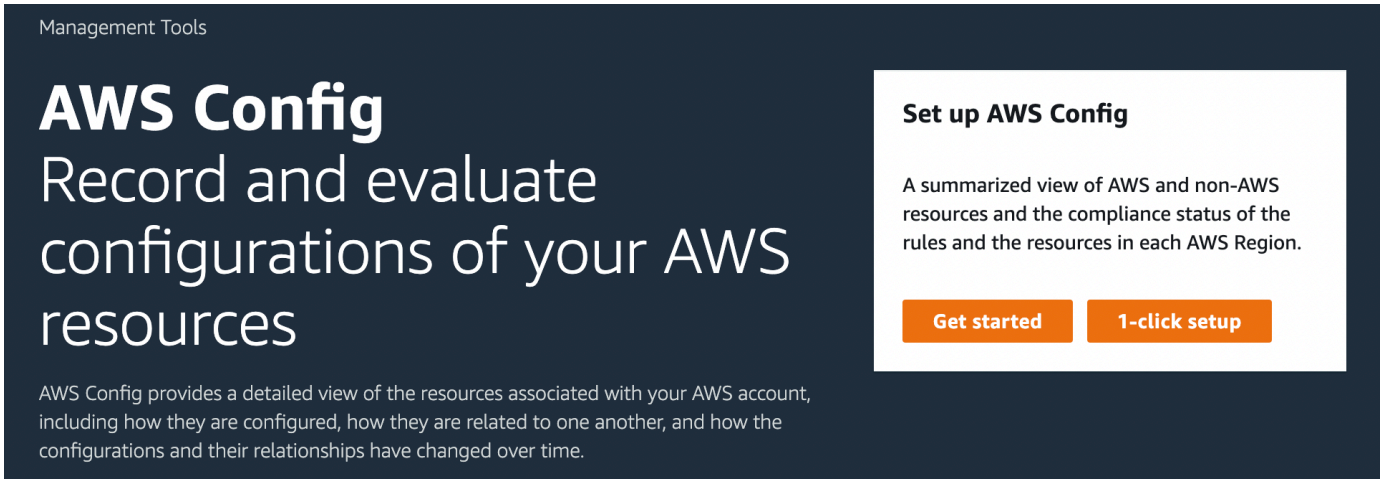
コンソール AWS Config で をセットアップする

AWS Management Console は、セットアップのための迅速かつ効率的なプロセスを提供します AWS Config。

設定

コンソール AWS Config で を設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. AWS Config コンソールを初めて開く場合、または新しいリージョン AWS Config で を設定する場合、 AWS Config コンソールページは次のようになります。



3. AWS ベストプラクティス AWS Config に基づいて、ワンクリックセットアップを選択して起動します。また、「使用開始」を選択して、より詳細なセットアッププロセスに進むこともできます。

トピック

- のワンクリックセットアップ AWS Config
- の手動セットアップ AWS Config

のワンクリックセットアップ AWS Config

AWS Config ワンクリック設定は、手動選択の数を減らすことで、 AWS Config コンソールのお客様の開始プロセスを簡素化するのに役立ちます。セットアッププロセスのすべての手動選択を確認するには、「「手動セットアップ」を参照してください。

ワンクリック設定を使用してコンソール AWS Config で を設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. [1-click setup] (ワンクリックセットアップ) を選択します。

セットアップページには 3 つのステップが含まれていますが、[1-click setup] (ワンクリックセットアップ) ワークフローでは、自動的にステップ 3 (レビュー) に誘導されます。次に、その手順の内訳を示します。

- 設定: AWS Config コンソールでリソースとロールを記録する方法を選択し、設定履歴と設定スナップショットファイルの送信先を選択します。
- ルール: この AWS リージョン サポート AWS Config ルールでは、このステップを使用して、アカウントに追加できる初期マネージドルールを設定できます。設定後、 AWS Config は選択したルールに照らして AWS リソースを評価します。追加のルールの作成や、既存のルールの更新は、設定後にアカウントで行うことができます。
- 確認: 設定の詳細を確認します。

ステップ 1: 設定

記録方法

記録するオプション カスタマイズ可能なオーバーライドを持つすべてのリソースタイプが選択されます。 AWS Config は、このリージョンで現在および将来サポートされているすべてのリソースタイプを記録します。詳細については、[サポートされるリソースタイプ] を参照してください。

- デフォルト設定

  デフォルトの記録頻度は [連続] に設定されています。つまり、 は、変更が発生するたびに設定の変更を継続的に AWS Config 記録します。

  AWS Config は、記録頻度を日次に設定するオプションもサポートしています。設定した後、このオプションを選択した場合、以前に記録された CI と異なる場合にのみ、過去 24 時間におけるリソースの最新の状態を表す設定項目 (CI) を、受け取ります。詳細については、「Recording Frequency」を参照してください。

  > **Note**
  >
  > AWS Firewall Manager は、リソースをモニタリングするために継続的な記録に依存します。Firewall Manager を使用している場合、記録頻度を連続に設定することをお勧めします。

- オーバーライド設定 - オプション

  設定した後、オプションで特定のリソースタイプの記録頻度を上書きしたり、特定のリソースタイプを記録から除外したりできます。デフォルト設定を上書きするには、 AWS Config コンソールの左側のナビゲーションで設定を選択し、編集を選択します。

リソースを記録する際の考慮事項

AWS Config 評価の数が多い

AWS Config での最初の月の記録中に、後続の月と比較して、アカウントのアクティビティが増加することがあります。最初のブートストラッププロセス中に、 は、 が記録 AWS Config するために選択したアカウント内のすべてのリソースで評価 AWS Config を実行します。

一時的なワークロードを実行している場合、これらの一時リソースの作成と削除に関連する設定の変更を記録するため、 AWS Config のアクティビティが増加する可能性があります。一時的なワークロードとは、必要なときにロードされて実行されるコンピューティングリソースを一時的に使用することです。例には、Amazon Elastic Compute Cloud (Amazon EC2) スポットインスタンス、Amazon EMR ジョブ、 AWS Auto Scalingがあります。一時的なワークロードの実行によるアクティビティの増加を避けたい場合は、これらのリソースタイプを記録から除外するよう設定レコーダーを設定するか、または AWS Config をオフにした別のアカウントでこの種のワークロードを実行し、設定の記録とルール評価の増加を回避することができます。

グローバルリソースタイプ | Aurora グローバルクラスターは、最初は記録に含められます

`AWS::RDS::GlobalCluster` リソースタイプは、設定レコーダーが有効になっているサポートされているすべての AWS Config リージョンに記録されます。

有効なすべてのリージョンで `AWS::RDS::GlobalCluster` を記録しない場合、設定後にこのリソースタイプを記録から除外できます。左のナビゲーションバーで、[設定] を選択し、[編集] を選択します。[編集] から、[記録方法] セクションの[オーバーライド設定] を選択し、`AWS::RDS::GlobalCluster` を選択してら、「記録から除外」のオーバーライドを選択します。

グローバルリソースタイプ | IAM リソースタイプは、最初は記録から除外されます。

コスト削減のため、「グローバルに記録されたすべての IAM リソースタイプ」は、最初は記録から除外されます。このバンドルには、IAM ユーザー、グループ、ロール、およびカスタマー管理ポリシーが含まれます。[削除] を選択してオーバーライドを削除し、これらのリソースを記録に含めます。

さらに、グローバル IAM リソースタイプ (`AWS::IAM::User`、`AWS::IAM::Group`、`AWS::IAM::Role`、および `AWS::IAM::Policy`) は、2022 年 2 月より後に AWS Config がサポートされるリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。

データガバナンス

このセクションでは、7 年間 (2557 日) データを保持するデフォルトの AWS Config データ保持期間が選択されています。

既存の AWS Config サービスにリンクされたロールを使用するオプションが選択され、 がAWS Config ロールに設定されます。サービスにリンクされたロールは によって事前定義 AWS Config されており、サービスが他の サービスを呼び出すために必要なすべてのアクセス許可が含まれています AWS 。

配信方法

このセクションでは、アカウントからバケットを選択するオプションが選択されています。この選択は、デフォルトで `config-bucket-accountid` 形式で名前が付けられたアカウントのバケットとなります。例えば、`config-bucket-012345678901`。その形式でバケットを作成していない場合は、自動的に作成されます。独自のバケットを作成する場合、「Amazon Simple Storage Service ユーザーガイド」の「バケットの作成」を参照してください。

S3 バケットの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「バケットの概要」を参照してください。

ステップ 2: ルール

AWS マネージド型ルールについては、このステップではルールは選択されていません。アカウントの設定が完了した後にルールを作成および更新することをお勧めします。

ステップ 3: 確認

AWS Config セットアップの詳細を確認します。戻って各セクションの変更を編集できます。確認 を選択してセットアップを完了します AWS Config。

の手動セットアップ AWS Config

開始方法ワークフローでは、セットアッププロセスのすべての手動選択を確認して、 AWS Config コンソールの使用を開始できます。簡単な開始プロセスについては、「ワンクリックセットアップ」を参照してください。

開始方法を使用して コンソール AWS Config で を設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。

2. [開始する] を選択します。

セットアップページには 3 つのステップがあります。以下に、[Get started] (使用開始) を選択した後の手順の内訳を示します。

- 設定: AWS Config コンソールでリソースとロールを記録する方法を選択し、設定履歴と設定スナップショットファイルの送信先を選択します。
- ルール: この AWS リージョン サポート AWS Config ルールでは、このステップを使用して、アカウントに追加できる初期マネージドルールを設定できます。設定後、 AWS Config は選択したルールに照らして AWS リソースを評価します。追加のルールを作成したり、既存のルールを更新したり、設定後にアカウントで更新できます。
- 確認: 設定の詳細を確認します。

ステップ 1: 設定

記録方法

[記録方法] セクションで、記録方法を選択します。 AWS Config 記録する AWS リソースを指定できます。

All resource types with customizable overrides

このリージョンで現在および今後サポートされているすべてのリソースタイプの設定変更を記録する AWS Config ように を設定します。特定のリソースタイプの記録頻度をオーバーライドしたり、特定のリソースタイプを記録から除外したりできます。詳細については、[サポートされるリソースタイプ] を参照してください。

- デフォルト設定

  現在および将来サポートされるすべてのリソースタイプについて、デフォルトの記録頻度を設定します。詳細については、「Recording Frequency」を参照してください。

  - 継続的な記録 – 変更が発生するたびに、設定の変更を継続的に記録 AWS Config します。
  - 日時記録 - 以前に記録された CI と異なる場合にのみ、過去 24 時間におけるリソースの最新の状態を表す設定項目 (CI) を、受け取ります。

> **Note**
>
> AWS Firewall Manager は、リソースをモニタリングするために継続的な記録に依存します。Firewall Manager を使用している場合、記録頻度を連続に設定することをお勧めします。

- 上書き設定

  特定のリソースタイプの記録頻度を上書きしたり、特定のリソースタイプを記録から除外したりします。リソースタイプの記録頻度を変更するか、またはリソースタイプの記録を停止した場合、既に記録されている設定項目は変更されません。

Specific resource types

指定したリソースタイプのみの設定変更を記録する AWS Config ように を設定します。

- 特定のリソースタイプ

  記録するリソースタイプとその頻度を選択します。詳細については、「Recording Frequency」を参照してください。

  - 継続的な記録 – 変更が発生するたびに、設定の変更を継続的に記録 AWS Config します。
  - 日時記録 - 以前に記録された CI と異なる場合にのみ、過去 24 時間におけるリソースの最新の状態を表す設定項目 (CI) を、受け取ります。

> **Note**
>
> AWS Firewall Manager は、リソースをモニタリングするために継続的な記録に依存します。Firewall Manager を使用している場合、記録頻度を連続に設定することをお勧めします。

リソースタイプの記録頻度を変更するか、またはリソースタイプの記録を停止した場合、既に記録されている設定項目は変更されません。

リソースを記録する際の考慮事項

AWS Config 評価の数が多い

AWS Config での最初の月の記録中に、後続の月と比較して、アカウントのアクティビティが増加することがあります。最初のブートストラッププロセス中に、 は、 が記録 AWS Config するために選択したアカウント内のすべてのリソースで評価 AWS Config を実行します。

一時的なワークロードを実行している場合、これらの一時リソースの作成と削除に関連する設定の変更を記録するため、 AWS Config のアクティビティが増加する可能性があります。一時的なワークロードとは、必要なときにロードされて実行されるコンピューティングリソースを一時的に使用することです。例としては、Amazon Elastic Compute Cloud (Amazon EC2) スポットインスタンス、Amazon EMR ジョブ、 AWS Auto Scalingなどがあります。一時的なワークロードの実行によるアクティビティの増加を避けたい場合は、これらのリソースタイプを記録から除外するよう設定レコーダーを設定するか、または AWS Config をオフにした別のアカウントでこの種のワークロードを実行し、設定の記録とルール評価の増加を回避することができます。

Considerations: All resource types with customizable overrides

グローバルに記録するリソースタイプ | Aurora グローバルクラスターは、最初は記録に含められます

`AWS::RDS::GlobalCluster` リソースタイプは、設定レコーダーが有効になっているサポートされているすべての AWS Config リージョンに記録されます。

すべての有効なリージョンで `AWS::RDS::GlobalCluster` を記録しない場合、「AWS RDS GlobalCluster」を選択し、「記録から除外する」というオーバーライドを選択します。

グローバルリソースタイプ | IAM リソースタイプは、最初は記録から除外されます。

コスト削減のため、グローバル IAM リソースタイプは、最初は記録から除外されます。このバンドルには、IAM ユーザー、グループ、ロール、およびカスタマー管理ポリシーが含まれます。[削除] を選択してオーバーライドを削除し、これらのリソースを記録に含めます。

さらに、グローバル IAM リソースタイプ (`AWS::IAM::User`、`AWS::IAM::Group`、`AWS::IAM::Role`、) は、2022 年 2 月 AWS Config 以降に でサポートされているリージョンでは記録`AWS::IAM::Policy`できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。

制限

最大 100 の頻度のオーバーライドと 600 の除外のオーバーライドを追加できます。

次のリソースタイプに日次記録を指定することはできません。

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

利用可能なリージョン

が追跡 AWS Config するリソースタイプを指定する前に、Resource Coverage by Region Availability をチェックして、リソースタイプがセットアップした AWS リージョンでサポートされているかどうかを確認します AWS Config。リソースタイプが少なくとも 1 つのリージョン AWS Config で でサポートされている場合は、指定したリソースタイプがセットアップしたリージョンでサポートされていない場合でも AWS Config、 でサポートされているすべての AWS リージョンでそのリソースタイプの記録を有効にできます AWS Config。

制限

すべてのリソースタイプが同じ頻度であれば制限はありません。少なくとも 1 つのリソースタイプが継続に設定されている場合、日次の頻度で最大 100 のリソースタイプを追加できます。

次のリソースタイプに日次頻度はサポートされていません。

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

データガバナンス

- データ保持期間では、デフォルトの保持期間を選択して AWS Config データを 7 年間 (2557) 保持するか、 によって記録された項目のカスタム保持期間を設定します AWS Config。

  AWS Config では、 の保持期間を指定してデータを削除できます`ConfigurationItems`。保持期間を指定すると、 AWS Config は `ConfigurationItems` を指定された期間保持します。最小 30 日から最大 7 年 (2557 日) の期間を選択できます。 は、指定した保持期間より古いデータ AWS Config を削除します。
- の IAM ロール AWS Configでは、アカウントから既存の AWS Config サービスにリンクされたロールまたは IAM ロールを選択します。

- サービスにリンクされたロールは によって事前定義 AWS Config されており、サービスが他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

> **Note**
>
> 推奨: サービスにリンクされたロールを使用する
> サービスにリンクされたロールを使用することをお勧めします。サービスにリンクされたロールは、 AWS Config が予想どおりに実行するのに必要なすべてのアクセス許可を追加します。

- それ以外の場合は、既存のロールとアクセス許可ポリシーの 1 つから IAM ロールを選択します。

> **Note**
>
> ポリシーとコンプライアンス結果
> で管理される IAM ポリシーやその他のポリシーは、 AWS Config がリソースの設定変更を記録するアクセス許可を持っているかどうかに影響を与える可能性があります。AWS Organizationsさらに、ルールはリソースの設定を直接評価し、ルールは評価の実行時にこれらのポリシーを考慮しません。有効なポリシーが、 の使用方法と一致していることを確認してください AWS Config。
> IAM ロール再利用時に最小限のアクティビティ許可を維持する
> や AWS Configなどの AWS Security Hub を使用する AWS サービスを使用し AWS Control Tower、IAM ロールがすでに作成されている場合は、セットアップ AWS Config 時に使用する IAM ロールが既存の IAM ロールと同じ最小限のアクセス許可を保持していることを確認してください。これを実行して、他の AWS サービスが期待どおりに実行されるようにする必要があります。
> たとえば、 に S3 オブジェクト AWS Config の読み取りを許可する IAM ロール AWS Control Tower がある場合、設定時に使用する IAM ロールに同じアクセス許可が付与されていることを確認してください AWS Config。そうしないと、 AWS Control Tower の動作に支障をきたす可能性があります。

配信方法

- [Delivery method] (配信方法) では、 AWS Config から設定履歴と設定スナップショットのファイルを送信する先の S3 バケットを選択します。

- [Create a bucket] (バケットの作成) — [S3 bucket name] (S3 バケット名) に S3 バケットの名前を入力します。

  Amazon S3 の既存のバケット名と重複しないように一意の名前を入力する必要があります。一意の名前にする 1 つの方法としては、組織の名前などをプレフィックスとして含めます。バケット名を作成後に変更することはできません。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「バケットの制約と制限」を参照してください。

- [Choose a bucket from your account] (アカウントからバケットを選択) – [S3 bucket name] (S3 バケット名) で目的のバケットを選択します。
- [Choose a bucket from another account] (別のアカウントからバケットを選択) — [S3 bucket name] (S3 バケット名) にバケット名を入力します。

> **Note**
>
> バケットのアクセス許可
> 別のアカウントからバケットを選択する場合、そのバケットにはアクセス許可を付与するポリシーが必要です AWS Config。詳細については、「AWS Config 配信チャネルの Amazon S3 バケットのアクセス許可」を参照してください。

- Amazon SNS トピックで、設定変更と通知を Amazon SNS トピックにストリームして、設定履歴配信、設定スナップショット配信、コンプライアンスなどの通知 AWS Config を送信するようにします。
- Amazon SNS AWS Config トピックにストリーミングすることを選択した場合は、ターゲットトピックを選択します。
  - [Create a topic] (トピックの作成) — [Topic Name] (トピック名) に SNS トピックの名前を入力します。
  - [Choose a topic from your account] (アカウントからトピックを選択) — [Topic Name] (トピック名) で目的のトピックを選択します。
  - [Choose a topic from another account] (別のアカウントからトピックを選択) – [Topic ARN] (トピック ARN) にトピックの Amazon リソースネーム (ARN) を入力します。別のアカウントからトピックを選択する場合、トピックにはアクセス許可を付与するポリシーが必要です AWS Config。詳細については、「Amazon SNS トピックへのアクセス許可」を参照してください。

> **Note**
>
> Amazon SNS トピックのリージョン

Amazon SNS トピックは、設定したリージョンと同じリージョンに存在する必要があります AWS Config。

ステップ 2: ルール

ルールをサポートするリージョン AWS Config で を設定する場合は、次へ を選択します。

ステップ 3: 確認

AWS Config セットアップの詳細を確認します。戻って各セクションの変更を編集できます。確認 を選択して設定を完了します AWS Config。

詳細情報

アカウント内の既存のリソースの検索とリソースの設定の理解については、「Looking up Resources」、「Viewing Compliance Informance」、「Viewing Compliance Informance」を参照してください。

Amazon Simple Queue Service を使用して AWS 、リソースをプログラムでモニタリングすることもできます。詳細については、「Amazon SQS による AWS リソース変更のモニタリング」を参照してください。

AWS Config で をセットアップする AWS CLI

AWS CLI は、 AWS のサービスを管理するための統合ツールです。ダウンロードと設定のツールを 1 つだけ使用すると、コマンドラインから複数の AWS サービスを制御したり、スクリプトを使用して自動化したりできます。の詳細 AWS CLI と AWS CLI ツールのインストール手順については、「AWS Command Line Interface ユーザーガイド」の以下を参照してください。

- AWS Command Line Interface ユーザーガイド
- AWS Command Line Interfaceのセットアップ

必要に応じて、 `aws configure`を入力して、 AWS Config が利用可能な AWS リージョンを使用する AWS CLI ように を設定します。

設定

AWS Config で をセットアップするには、以下のトピックを参照してください AWS CLI。

トピック

- AWS Config で をセットアップするための前提条件 AWS CLI
- を使用したカスタマーマネージド設定レコーダー AWS Config から開始する AWS CLI
- AWS Config が正常に開始されたことを確認する AWS CLI

AWS Config で をセットアップするための前提条件 AWS CLI

AWS で を設定する前に AWS CLI、前提条件として Amazon S3 バケット、Amazon SNS トピック、およびポリシーがアタッチされた IAM ロールを作成する必要があります。その後、 を使用してバケット、トピック、ロール AWS CLI を指定できます AWS Config。次の手順に従って、 AWS Configの前提条件をセットアップします。

トピック

- ステップ 1: Amazon S3 バケットを作成する
- ステップ 2: Amazon SNS トピックを作成する
- ステップ 3: IAM ロールを作成する

ステップ 1: Amazon S3 バケットを作成する

アカウントに Amazon S3 バケットが既にあり、それを使用する場合は、このステップをスキップして ステップ 2: Amazon SNS トピックを作成する に進んでください。

S3 コンソールの使用

バケットを作成するには

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [バケットの作成] を選択します。
3. [バケット名] に、バケットの DNS に準拠する名前を入力します。

   バケット名には次の条件があります。

   - すべての Amazon S3 で一意にする。
   - 3 ~ 63 文字で指定する。
   - 大文字を含めないでください。
   - 先頭の文字には小文字の英文字または数字を使用する。

バケットを作成したら、その名前を変更することはできません。バケット名は、Amazon S3 の既存のバケット名と重複しないように指定してください。バケットの命名ルールと変換の詳細については、「Amazon Simple Storage Service デベロッパーガイド」のバケットの制約と制限を参照してください。

> **Important**
>
> バケット名に機密情報を含めないでください。バケット名は、バケット内のオブジェクトを参照する URL に表示されます。

4. リージョンで、バケットを配置する AWS リージョンを選択します。

   レイテンシーとコストを最小化するため、さらに規制条件に対応するために、最寄りのリージョンを選択します。明示的に別のリージョンに移動する場合を除き、特定のリージョンに保管されたオブジェクトは、そのリージョンから移動されることはありません。Amazon S3 AWS Regions のリストについては、のAWS 「サービスエンドポイント」を参照してくださいAmazon Web Services 全般のリファレンス。

5. ブロックパブリックアクセスのバケット設定 で、バケットに適用するパブリックアクセスブロック設定を選択します。

   パブリックウェブサイトをホスティングする場合など、ユースケースでオフにする必要のある設定が 1 つ以上あることがわかっている場合を除いて、すべての設定を有効にしておくことをお勧めします。バケットに対して有効にしたパブリックアクセスブロック設定は、バケットに作成するすべてのアクセスポイントに対しても有効になります。パブリックアクセスのブロックの詳細については、「Amazon Simple Storage Service 開発者ガイド」の「Amazon S3 パブリックアクセスブロックの使用」を参照してください。

6. (オプション) S3 オブジェクトロックを有効にする場合:

   a. [詳細設定] を選択し、表示されるメッセージを読みます。

   > **Important**
   >
   > バケットに対する S3 オブジェクトロックは、バケットの作成時にのみ有効にできます。バケットに対してオブジェクトロックを有効にした場合、後で無効にすることはできません。バケットに対してオブジェクトロックを有効にすると、バージョニングも有効になります。バケットに対してオブジェクトロックを有効にした後、バケット内のオブジェクトを保護するには、オブジェクトロック設定を定義する必

要があります。オブジェクトの保護の設定の詳細については、「Amazon S3 コンソールを使用した S3 オブジェクトロックの設定」を参照してください。

b. オブジェクトロックを有効にする場合は、テキストボックスに「enable」と入力し、[確認] を選択します。

S3 オブジェクトロック機能の詳細については、「Amazon Simple Storage Service 開発者ガイド」の「Amazon S3 オブジェクトロックを使用したオブジェクトのロック」を参照してください。

7. [バケットを作成] を選択します。

AWS SDKsの使用

AWS SDKs を使用してバケットを作成する場合は、クライアントを作成し、そのクライアントを使用してバケットを作成するリクエストを送信する必要があります。ベストプラクティスとして、クライアントとバケットを同じ AWS リージョンで作成する必要があります。クライアントまたはバケットの作成時にリージョンを指定しない場合、Amazon S3 ではデフォルトのリージョンである米国東部 (バージニア北部) が使用されます。

デュアルスタックエンドポイントにアクセスするクライアントを作成するには、 を指定する必要があります AWS リージョン。詳細については、Amazon S3 デュアルスタックのエンドポイントを参照してください。利用可能な のリストについては AWS リージョン、『』の「リージョンとエンドポイント」を参照してくださいAWS 全般のリファレンス。

クライアントを作成すると、リージョンはリージョン固有のエンドポイントにマッピングされます。クライアントは、このエンドポイントを使用して Amazon S3 と通信します。`s3.<region>.amazonaws.com`。リージョンがローンチされたのが 2019 年 3 月 20 日以降である場合は、クライアントとバケットは同じリージョン内にある必要があります。2019 年 3 月 20 日以前にローンチされたリージョンの場合は、米国東部 (バージニア北部) のリージョンでクライアントを使用することによりバケットを作成できます。詳細については、「レガシーエンドポイント」を参照してください。

これらの AWS SDK コード例は、次のタスクを実行します。

- AWS リージョンを明示的に指定してクライアントを作成する - この例では、クライアントは `s3.us-west-2.amazonaws.com` エンドポイントを使用して Amazon S3 と通信します。任意の AWS リージョンを指定できます。のリストについては AWS リージョン、「 AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。

- バケット名のみを指定してバケット作成リクエストを送信する - クライアントが Amazon S3 にリクエストを送信し、クライアントが作成されたリージョンにバケットを作成します。
- バケットの場所情報を取得する - Amazon S3 が、バケットの場所情報を、そのバケットに関連付けられている場所のサブリソースに保存します。

次のサンプルコードは、`CreateBucket` を使用する方法を説明しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
        /// <summary>
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
```

```
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
                return false;
            }
        }
```

オブジェクトロックを有効にしてバケットを作成します。

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「CreateBucket」を参照してください。

Bash

AWS CLI Bash スクリプトを使用する

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
```

```
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
```

```
    usage
    return 1
  fi

  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「CreateBucket」を参照してください。

C++

SDK for C++

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
bool AwsDoc::S3::createBucket(const Aws::String &bucketName,
                              const Aws::S3::S3ClientConfiguration &clientConfig)
 {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: createBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    } else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- API の詳細については、「AWS SDK for C++ API リファレンス」の「CreateBucket」を参照してください。

CLI

AWS CLI

例 1: バケットを作成するには

次の create-bucket の例は、amzn-s3-demo-bucket という名前のバケットを作成します。

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1
```

出力:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

詳細については、「Amazon S3 ユーザーガイド」の「バケットの作成」を参照してください。

例 2: 所有者の強制を使用してバケットを作成するには

次の create-bucket の例は、S3 オブジェクトの所有権のバケット所有者の強制設定を使用して、amzn-s3-demo-bucket という名前のバケットを作成します。

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

出力:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

詳細については、Amazon S3 ユーザーガイドのオブジェクトの所有権のコントロールと ACL の無効化を参照してください。

例 3: ``us-east-1`` リージョンの外にバケットを作成するには

次の `create-bucket` の例は、`eu-west-1` リージョンに `amzn-s3-demo-bucket` という名前のバケットを作成します。`us-east-1` の外にある目的のリージョンにバケットを作成するには、適切な `LocationConstraint` を指定する必要があります。

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

出力:

```
{
    "Location": "http://amzn-s3-demo-bucket.s3.amazonaws.com/"
}
```

詳細については、「Amazon S3 ユーザーガイド」の「バケットの作成」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「CreateBucket」を参照してください。

Go

SDK for Go V2

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

デフォルト設定を使用してバケットを作成します。

```
import (
 "bytes"
```

```
 "context"
 "errors"
 "fmt"
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(ctx context.Context, name string, region
 string) error {
 _, err := basics.S3Client.CreateBucket(ctx, &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", name)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", name)
```

```
    err = exists
   }
  } else {
   err = s3.NewBucketExistsWaiter(basics.S3Client).Wait(
    ctx, &s3.HeadBucketInput{Bucket: aws.String(name)}, time.Minute)
   if err != nil {
    log.Printf("Failed attempt to wait for bucket %s to exist.\n", name)
   }
  }
  return err
}
```

オブジェクトロックを使用してバケットを作成し、作成が完了するまで待ちます。

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// S3Actions wraps S3 service actions.
type S3Actions struct {
 S3Client  *s3.Client
 S3Manager *manager.Uploader
}



// CreateBucketWithLock creates a new S3 bucket with optional object locking
 enabled
// and waits for the bucket to exist before returning.
```

```
func (actor S3Actions) CreateBucketWithLock(ctx context.Context, bucket string,
 region string, enableObjectLock bool) (string, error) {
 input := &s3.CreateBucketInput{
  Bucket: aws.String(bucket),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 }

 if enableObjectLock {
  input.ObjectLockEnabledForBucket = aws.Bool(true)
 }

 _, err := actor.S3Client.CreateBucket(ctx, input)
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", bucket)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", bucket)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(actor.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(bucket)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", bucket)
  }
 }

 return bucket, err
}
```

- API の詳細については、「AWS SDK for Go API リファレンス」の「CreateBucket」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

バケットを作成します。

```
    /**
     * Creates an S3 bucket asynchronously.
     *
     * @param bucketName the name of the S3 bucket to create
     * @return a {@link CompletableFuture} that completes when the bucket is
created and ready
     * @throws RuntimeException if there is a failure while creating the bucket
     */
    public CompletableFuture<Void> createBucketAsync(String bucketName) {
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .build();

        CompletableFuture<CreateBucketResponse> response =
getAsyncClient().createBucket(bucketRequest);
        return response.thenCompose(resp -> {
            S3AsyncWaiter s3Waiter = getAsyncClient().waiter();
            HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
                .bucket(bucketName)
                .build();

            CompletableFuture<WaiterResponse<HeadBucketResponse>>
waiterResponseFuture =
                s3Waiter.waitUntilBucketExists(bucketRequestWait);
            return waiterResponseFuture.thenAccept(waiterResponse -> {
                waiterResponse.matched().response().ifPresent(headBucketResponse
-> {
                    logger.info(bucketName + " is ready");
                });
            });
```

```
        }).whenComplete((resp, ex) -> {
            if (ex != null) {
                throw new RuntimeException("Failed to create bucket", ex);
            }
        });
    }
```

オブジェクトロックを有効にしてバケットを作成します。

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
 bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();

        getClient().createBucket(bucketRequest);
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「CreateBucket」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

バケットを作成します。

```
import {
  BucketAlreadyExists,
  BucketAlreadyOwnedByYou,
  CreateBucketCommand,
  S3Client,
  waitUntilBucketExists,
} from "@aws-sdk/client-s3";

/**
 * Create an Amazon S3 bucket.
 * @param {{ bucketName: string }} config
 */
export const main = async ({ bucketName }) => {
  const client = new S3Client({});

  try {
    const { Location } = await client.send(
      new CreateBucketCommand({
        // The name of the bucket. Bucket names are unique and have several other
 constraints.
        // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
        Bucket: bucketName,
      }),
    );
    await waitUntilBucketExists({ client }, { Bucket: bucketName });
    console.log(`Bucket created with location ${Location}`);
  } catch (caught) {
    if (caught instanceof BucketAlreadyExists) {
      console.error(
        `The bucket "${bucketName}" already exists in another AWS account. Bucket
 names must be globally unique.`,
      );
    }
    // WARNING: If you try to create a bucket in the North Virginia region,
    // and you already own a bucket in that region with the same name, this
    // error will not be thrown. Instead, the call will return successfully
    // and the ACL on that bucket will be reset.
    else if (caught instanceof BucketAlreadyOwnedByYou) {
      console.error(
        `The bucket "${bucketName}" already exists in this AWS account.`,
      );
```

```
    } else {
      throw caught;
    }
  }
};
```

- 詳細については、「AWS SDK for JavaScript デベロッパーガイド」を参照してください。
- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「CreateBucket」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client.fromEnvironment { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「CreateBucket」を参照してください。

PHP

SDK for PHP

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

バケットを作成します。

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);

        try {
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
$exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- API の詳細については、「AWS SDK for PHP API リファレンス」の「CreateBucket」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

デフォルトの設定でバケットを作成します。

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
        """
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

ライフサイクル設定を使用してバージョン対応バケットを作成します。

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
```

```
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
 expiration},
                    }
                ]
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「CreateBucket」を参照してください。

Ruby

SDK for Ruby

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                  create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
```

```
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

- API の詳細については、「AWS SDK for Ruby API リファレンス」の「CreateBucket」を参照してください。

Rust

SDK for Rust

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
pub async fn create_bucket(
    client: &aws_sdk_s3::Client,
    bucket_name: &str,
    region: &aws_config::Region,
) -> Result<Option<aws_sdk_s3::operation::create_bucket::CreateBucketOutput>,
 S3ExampleError> {
```

```
    let constraint =
 aws_sdk_s3::types::BucketLocationConstraint::from(region.to_string().as_str());
    let cfg = aws_sdk_s3::types::CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    let create = client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await;

    // BucketAlreadyExists and BucketAlreadyOwnedByYou are not problems for this
 task.
    create.map(Some).or_else(|err| {
        if err
            .as_service_error()
            .map(|se| se.is_bucket_already_exists() ||
 se.is_bucket_already_owned_by_you())
            == Some(true)
        {
            Ok(None)
        } else {
            Err(S3ExampleError::from(err))
        }
    })
}
```

- API の詳細については、「AWS SDK for Rust API リファレンス」の「CreateBucket」を参照してください。

SAP ABAP

SDK for SAP ABAP

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
    TRY.
        " determine our region from our session
        DATA(lv_region) = CONV /aws1/s3_bucketlocationcnstrnt( lo_session-
>get_region( ) ).
        DATA lo_constraint TYPE REF TO /aws1/cl_s3_createbucketconf.
        " When in the us-east-1 region, you must not specify a constraint
        " In all other regions, specify the region as the constraint
        IF lv_region = 'us-east-1'.
          CLEAR lo_constraint.
        ELSE.
          lo_constraint = NEW /aws1/cl_s3_createbucketconf( lv_region ).
        ENDIF.

        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
            io_createbucketconfiguration  = lo_constraint ).
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- API の詳細については、「AWS SDK for SAP ABAP API リファレンス」の「CreateBucket」を参照してください。

Swift

SDK for Swift

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import AWSS3

    public func createBucket(name: String) async throws {
        var input = CreateBucketInput(
```

```
            bucket: name
        )

        // For regions other than "us-east-1", you must set the
 locationConstraint in the createBucketConfiguration.
        // For more information, see LocationConstraint in the S3 API guide.
        // https://docs.aws.amazon.com/AmazonS3/latest/API/
API_CreateBucket.html#API_CreateBucket_RequestBody
        if let region = configuration.region {
            if region != "us-east-1" {
                input.createBucketConfiguration =
 S3ClientTypes.CreateBucketConfiguration(locationConstraint:
 S3ClientTypes.BucketLocationConstraint(rawValue: region))
            }
        }

        do {
            _ = try await client.createBucket(input: input)
        }
        catch let error as BucketAlreadyOwnedByYou {
            print("The bucket '\(name)' already exists and is owned by you. You
 may wish to ignore this exception.")
            throw error
        }
        catch {
            print("ERROR: ", dump(error, name: "Creating a bucket"))
            throw error
        }
    }
```

- API の詳細については、AWS SDK for Swift API リファレンスの「CreateBucket」を参照してください。

> **Note**
>
> 別のアカウントの Amazon S3 バケットを使用することもできますが、 AWS Configに対してアクセス許可を付与するバケットポリシーの作成が必要になる場合があります。Amazon S3 バケットへのアクセス許可を付与する方法については、AWS Config 配信チャネルの Amazon S3 バケットのアクセス許可 と ステップ 2: Amazon SNS トピックを作成する を順に参照してください。

ステップ 2: Amazon SNS トピックを作成する

アカウントに Amazon SNS トピックが既にあり、それを使用する場合は、このステップをスキップして「ステップ 3: IAM ロールを作成する」に進んでください。

SNS コンソールの使用

Amazon SNS トピックを作成するには

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. 次のいずれかを行います：
   - AWS アカウント 以前に でトピックを作成したことがない場合は、ホームページの Amazon SNS の説明をお読みください。
   - AWS アカウント 以前に でトピックが作成されている場合は、ナビゲーションパネルでトピックを選択します。
3. [トピック] ページで、[トピックの作成] を選択します。
4. [サブスクリプションの作成] ページで [詳細] セクションで、以下を実行します。
   a. [タイプ] で、トピックタイプ (標準またはFIFO) を選択します。
   b. トピックの名前を入力します。FIFO トピックで、名前の末尾に .fifo を追加します。
   c. (オプション) トピックの表示名を入力します。
   d. (オプション) FIFO トピックで、[コンテンツベースのメッセージ重複排除] を選択して、デフォルトのメッセージの重複排除を有効にします。詳細については、「FIFO トピックのメッセージ重複除外」を参照してください。
5. (オプション) [暗号化] セクションを展開し、以下の操作を実行します。詳細については、「保管時の暗号化」を参照してください。
   a. [暗号化の有効化] を選択します。
   b. カスタマーマスターキー (CMK) を指定します。詳細については、重要な用語を参照してください。

      CMK タイプごとに、[説明]、[アカウント]、および [CMK ARN] が表示されます。

> **Important**
>
> CMK の所有者ではない場合、または `kms:ListAliases` および `kms:DescribeKey` アクセス権限がないアカウントでログインしている場合、Amazon SNS コンソールで CMK に関する情報は表示できません。CMK の所有者に、これらのアクセス権限を付与するよう依頼します。詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS API アクセス権限: アクションとリソースのリファレンス」を参照してください。

- Amazon SNS （デフォルト) alias/aws/sns の AWS マネージド CMK はデフォルトで選択されています。

  > **Note**
  >
  > 以下に留意してください。
  >
  > - AWS Management Console を使用してトピックの Amazon SNS の AWS マネージド CMK を初めて指定すると、 は Amazon SNS の AWS マネージド CMK AWS KMS を作成します。
  > - または、SSE が有効になっているトピックで `Publish`アクションを初めて使用すると、 は Amazon SNS の AWS マネージド CMK AWS KMS を作成します。

- からカスタム CMK を使用するには AWS アカウント、カスタマーマスターキー (CMK) フィールドを選択し、リストからカスタム CMK を選択します。

  > **Note**
  >
  > カスタム CMK の作成手順については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

- AWS アカウント または別の AWS アカウントからカスタム CMK ARN を使用するには、カスタマーマスターキー (CMK) フィールドに入力します。

6. (オプション) デフォルトでは、トピックの所有者のみがトピックを発行またはサブスクライブできます。追加のアクセス許可を設定するには、[アクセスポリシー] セクションを展開します。詳

細については、「Amazon SNS におけるアイデンティティとアクセス管理」および「Amazon SNS のアクセス制御のケース例」を参照してください。

> **Note**
>
> コンソールを使用してトピックを作成すると、デフォルトのポリシーでは `aws:SourceOwner` 条件キーが使用されます。このキーは `aws:SourceAccount` に類似しています。

7. (オプション) 失敗したメッセージ配信試行を Amazon SNS で再試行する方法を設定するには、[配信再試行ポリシー (HTTP/S)] セクションを展開します。詳細については、「Amazon SNS メッセージ配信の再試行」を参照してください。
8. (オプション) CloudWatch へのメッセージの配信を Amazon SNS でログに記録する方法を設定するには、[配信ステータスのログ記録] セクションを展開します。詳細については、「メッセージの配信ステータスの Amazon SNS アプリケーション属性を使用する」を参照してください。
9. (オプション) トピックにメタデータタグを追加するには、[タグ] セクションを展開し、[キー] と [値] (オプション) に入力し、[タグの追加] を選択します。詳細については、「Amazon SNS トピックのタグ付け」を参照してください。
10. [トピックの作成] を選択してください。

    トピックが作成され、[***MyTopic***] ページが表示されます。

    トピックの名前、ARN、(オプション) 表示名、およびトピックの所有者の AWS アカウント ID が [Details] (詳細) セクションに表示されます。
11. トピック ARN をクリップボードにコピーします。例:

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

E メールアドレスを Amazon SNS トピックにサブスクライブするには

1. Amazon SNS コンソールのhttps://console.aws.amazon.com/sns/v3/homeを開いてください。
2. 左のナビゲーションペインで、[サブスクリプション] を選択します。
3. [サブスクリプション] ページで [サブスクリプションの作成] を選択します。
4. [サブスクリプションの作成] ページで [詳細] セクションで、以下を実行します。

    a. [トピック ARN] は、トピックの Amazon リソースネーム (ARN) を選択します。

b. [プロトコル] でエンドポイントタイプを選択します。使用可能なエンドポイントタイプは次のとおりです。

- HTTP/HTTPS
- Email/Email-JSON
- Amazon Data Firehose
- Amazon SQS

> **Note**
> SNS FIFO トピックにサブスクライブするには、このオプションを選択します。

- AWS Lambda
- プラットフォームアプリケーションエンドポイント
- SMS

c. [エンドポイント] に、エンドポイント値 (E メールアドレスや Amazon SQS キューの ARN など) を入力します。

d. Firehose エンドポイントのみ: [サブスクリプションロール ARN] で、Firehose 配信ストリームに書き込むために作成した IAM ロールの ARN を指定します。詳細については、「Prerequisites for subscribing Firehose delivery streams to Amazon SNS topics」を参照してください。

e. (オプション) Firehose、Amazon SQS、HTTP/S エンドポイントは、raw メッセージ配信を有効にすることもできます。詳細については、「Amazon SNS raw メッセージ配信」を参照してください。

f. (オプション) フィルターポリシーを設定するには、[サブスクリプションのフィルターポリシー] セクションを展開します。詳細については、「Amazon SNS サブスクリプションフィルターポリシー」を参照してください。

g. (オプション) サブスクリプションのデッドレターキューを設定するには、Redrive ポリシー (デッドレターキュー) を展開します。詳細については、「Amazon SNS デッドレターキュー (DLQ)」を参照してください。

h. [サブスクリプションの作成] を選択します。

   コンソールがサブスクリプションを作成し、サブスクリプションの [詳細] ページを開きます。

AWS SDKsの使用

AWS SDK を使用するには、認証情報を使用して SDK を設定する必要があります。詳細については、「AWS SDK とツールのリファレンスガイド」の「共有設定ファイルと認証情報ファイル」を参照してください。

次のサンプルコードは、`CreateTopic` を使用する方法を説明しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

トピックを作成して、個別の名前を付けます。

```
using System;
using System.Threading.Tasks;
using Amazon.SimpleNotificationService;
using Amazon.SimpleNotificationService.Model;

/// <summary>
/// This example shows how to use Amazon Simple Notification Service
/// (Amazon SNS) to add a new Amazon SNS topic.
/// </summary>
public class CreateSNSTopic
{
    public static async Task Main()
    {
        string topicName = "ExampleSNSTopic";

        IAmazonSimpleNotificationService client = new
AmazonSimpleNotificationServiceClient();

        var topicArn = await CreateSNSTopicAsync(client, topicName);
        Console.WriteLine($"New topic ARN: {topicArn}");
    }
```

```
        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

名前と特定の FIFO および重複除外属性を使用して新しいトピックを作成します。

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
        };
```

```
        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }

            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
"true");
            }
        }

        var createResponse = await
_amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「CreateTopic」を参照してください。

C++

SDK for C++

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
/*!
```

```
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }

    return outcome.IsSuccess();
}
```

- API の詳細については、「AWS SDK for C++ API リファレンス」の「CreateTopic」を参照してください。

CLI

AWS CLI

SNS トピックを作成するには

次の create-topic の例では、my-topic という名前の SNS トピックを作成します。

```
aws sns create-topic \
    --name my-topic
```

出力:

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

詳細については、AWS 「コマンドラインインターフェイスユーザーガイド」のAmazon SQS および Amazon SNS でのコマンドラインインターフェイスの使用」を参照してください。AWS

- API の詳細については、「AWS CLI コマンドリファレンス」の「CreateTopic」を参照してください。

Go

SDK for Go V2

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/sns"
 "github.com/aws/aws-sdk-go-v2/service/sns/types"
```

```
)

// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}



// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(ctx context.Context, topicName string,
 isFifoTopic bool, contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(ctx, &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- API の詳細については、AWS SDK for Go API リファレンスの「CreateTopic」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }
```

```
        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「CreateTopic」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。完全な例を見つけて、AWS コード例リポジトリでの設定と実行の方法を確認してください。

別のモジュールでクライアントを作成し、エクスポートします。

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

SDK モジュールとクライアントモジュールをインポートし、API を呼び出します。

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- 詳細については、AWS SDK for JavaScript デベロッパーガイドを参照してください。
- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「CreateTopic」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient.fromEnvironment { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「CreateTopic」を参照してください。

PHP

SDK for PHP

> **Note**
>
> GitHub には、その他のリソースもあります。完全な例を見つけて、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
```

```
use Aws\Sns\SnsClient;


/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- 詳細については、AWS SDK for PHP デベロッパーガイドを参照してください。
- API の詳細については、「AWS SDK for PHP API リファレンス」の「CreateTopic」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource


    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「CreateTopic」を参照してください。

Ruby

SDK for Ruby

> **Note**
>
> GitHub には、その他のリソースもあります。完全な例を見つけて、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = 'YourTopicName' # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
```

```
  unless sns_topic_creator.create_topic(topic_name)
    puts 'The topic was not created. Stopping program.'
    exit 1
  end
end
```

- 詳細については、AWS SDK for Ruby デベロッパーガイドを参照してください。
- API の詳細については、「AWS SDK for Ruby API リファレンス」の「CreateTopic」を参照してください。

Rust

SDK for Rust

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- API の詳細については、「AWS SDK for Rust API リファレンス」の「CreateTopic」を参照してください。

SAP ABAP

SDK for SAP ABAP

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
   TRY.
       oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
is returned for testing purposes. "
       MESSAGE 'SNS topic created' TYPE 'I'.
     CATCH /aws1/cx_snstopiclimitexcdex.
       MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
   ENDTRY.
```

- API の詳細については、AWS SDK for SAP ABAP API リファレンスの「CreateTopic」を参照してください。

Swift

SDK for Swift

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import AWSSNS

        let config = try await SNSClient.SNSClientConfiguration(region: region)
        let snsClient = SNSClient(config: config)

        let output = try await snsClient.createTopic(
            input: CreateTopicInput(name: name)
```

```
        )

        guard let arn = output.topicArn else {
            print("No topic ARN returned by Amazon SNS.")
            return
        }
```

- API の詳細については、 AWS SDK for Swift API リファレンスの「CreateTopic」を参照してください。

> **Note**
>
> 別のアカウントの Amazon SNS トピックを使用することもできますが、その場合は、 AWS Configに対するアクセス許可を付与するトピックポリシーの作成が必要になる場合があります。Amazon SNS トピックへのアクセス許可を付与する方法については、Amazon SNS トピックへのアクセス許可 と ステップ 3: IAM ロールを作成する を順に参照してください。

ステップ 3: IAM ロールを作成する

> **Important**
>
> （推奨) AWS Config サービスにリンクされたロールを使用する
> AWS Config サービスにリンクされたロール を使用することをお勧めします`AWSServiceRoleForConfig`。サービスにリンクされたロールは事前定義されており、が他の を呼び出す AWS Config ために必要なすべてのアクセス許可が含まれています AWS のサービス。 AWS Config サービスにリンクされたロールは、サービスにリンクされた設定レコーダーに必要です。
> 詳細については、「AWS Config用のサービスリンクロールの使用」を参照してください。

IAM コンソールの使用

IAM コンソールを使用して、Amazon S3 バケットへのアクセス、Amazon SNS トピックへのアクセス、サポートされている AWS リソースの設定詳細を取得するアクセス AWS Config 許可を付与する IAM ロールを作成できます。コンソールを使用して IAM ロールを作成すると、 AWS Config はロールに必要なアクセス許可を自動的に適用します。

> **Note**
>
> を使用する AWS サービス AWS Config （ AWS Security Hub や AWS Control Tower など) を使用していて、 AWS Config ロールがすでに作成されている場合は、他の AWS サービスが期待どおりに実行されるように、セットアップ時に使用する IAM ロールが、既に作成された AWS Config ロールと同じ最小権限 AWS Config を保持していることを確認する必要があります。
> 例えば、 AWS Control Tower に Amazon S3 オブジェクト AWS Config の読み取りを許可する IAM ロールがある場合、セットアップ時に使用する IAM ロール内で同じアクセス許可が付与されていることを確認する必要があります AWS Config。そうしないと、 AWS Control Tower のオペレーションが妨げられる可能性があります。
> の IAM ロールの詳細については AWS Config、AWS 「Identity and Access Management」を参照してください。

AWS サービスのロールを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. [Select trusted entity] (信頼されたエンティティの選択) で、[AWS のサービス] を選択します。
4. 目的のユースケースを選択します AWS Config。Config - カスタマイズ可能、Config - 組織、Config、または Config - コンフォーマンスパック。[次へ] を選択します。
5. [Name, review, and create] (名前、確認、および作成) ページで、ロールの詳細を確認し、[Create Role] (ロールの作成) を選択します。

AWS SDKsの使用

AWS SDK を使用するには、認証情報を使用して SDK を設定する必要があります。詳細については、「AWS SDK とツールのリファレンスガイド」の「共有設定ファイルと認証情報ファイル」を参照してください。

次のサンプルコードは、`CreateRole` を使用する方法を説明しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role.</param>
    /// <param name="rolePolicyDocument">The name of the IAM policy document
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
rolePolicyDocument)
    {
        var request = new CreateRoleRequest
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「CreateRole」を参照してください。

Bash

AWS CLI Bash スクリプトを使用する

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
```

```
  echo "  -n role_name   The name of the IAM role."
  echo "  -p policy_json -- The assume role policy document."
  echo ""
}

# Retrieve the calling parameters.
while getopts "n:p:h" option; do
  case "${option}" in
    n) role_name="${OPTARG}" ;;
    p) policy_document="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$role_name" ]]; then
  errecho "ERROR: You must provide a role name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$policy_document" ]]; then
  errecho "ERROR: You must provide a policy document with the -p parameter."
  usage
  return 1
fi

response=$(aws iam create-role \
  --role-name "$role_name" \
  --assume-role-policy-document "$policy_document" \
  --output text \
  --query Role.Arn)

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
```

```
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「CreateRole」を参照してください。

C++

SDK for C++

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;

    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
```

```
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- API の詳細については、「AWS SDK for C++ API リファレンス」の「CreateRole」を参照してください。

CLI

AWS CLI

例 1: IAM ロールを作成するには

次の `create-role` コマンドは、`Test-Role` という名前のロールを作成し、それに信頼ポリシーをアタッチします。

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

出力:

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

信頼ポリシーは、Test-Role-Trust-Policy.json ファイル内で JSON ドキュメントとして定義されます。(ファイル名と拡張子には意味はありません。) 信頼ポリシーはプリンシパルを指定する必要があります。

アクセス許可ポリシーをロールにアタッチするには、put-role-policy コマンドを使用します。

詳細については、「AWS IAM ユーザーガイド」の「IAM ロールの作成」を参照してください。

例 2: 最大セッション期間を指定して IAM ロールを作成するには

次の create-role コマンドは、Test-Role という名前のロールを作成し、最大セッション時間を 7,200 秒 (2 時間) に設定します。

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

出力:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

詳細については、AWS IAM ユーザーガイドの「ロールの最大セッション期間 (AWS API) の変更」を参照してください。

例 3: タグを使用して IAM ロールを作成するには

次のコマンドは、タグを使用して IAM ロール `Test-Role` を作成します。この例では、次の JSON 形式のタグを持つ `--tags` パラメータフラグを使用します: `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`。あるいは、`--tags` フラグを次の短縮形式のタグとともに使用することもできます: `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`。

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

出力:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
```

```
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

詳細については、「AWS IAM ユーザーガイド」で「IAM ロールのタグ付け」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「CreateRole」を参照してください

Go

SDK for Go V2

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/iam"
 "github.com/aws/aws-sdk-go-v2/service/iam/types"
)

// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
```

```
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(ctx context.Context, roleName string,
 trustedUserArn string) (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version: "2012-10-17",
  Statement: []PolicyStatement{{
   Effect:    "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
   Action:    []string{"sts:AssumeRole"},
  }},
 }
 policyBytes, err := json.Marshal(trustPolicy)
 if err != nil {
  log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
 trustedUserArn, err)
  return nil, err
 }
 result, err := wrapper.IamClient.CreateRole(ctx, &iam.CreateRoleInput{
  AssumeRolePolicyDocument: aws.String(string(policyBytes)),
  RoleName:                 aws.String(roleName),
 })
 if err != nil {
  log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
 } else {
  role = result.Role
 }
 return role, err
}
```

- API の詳細については、「AWS SDK for Go API リファレンス」の「CreateRole」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
                    rolename - The name of the role to create.\s
```

```
                    fileLocation - The location of the JSON document that
represents the trust policy.\s
               """;

       if (args.length != 2) {
           System.out.println(usage);
           System.exit(1);
       }

       String rolename = args[0];
       String fileLocation = args[1];
       Region region = Region.AWS_GLOBAL;
       IamClient iam = IamClient.builder()
               .region(region)
               .build();

       String result = createIAMRole(iam, rolename, fileLocation);
       System.out.println("Successfully created user: " + result);
       iam.close();
   }

   public static String createIAMRole(IamClient iam, String rolename, String
fileLocation) throws Exception {
       try {
           JSONObject jsonObject = (JSONObject)
readJsonSimpleDemo(fileLocation);
           CreateRoleRequest request = CreateRoleRequest.builder()
                   .roleName(rolename)
                   .assumeRolePolicyDocument(jsonObject.toJSONString())
                   .description("Created using the AWS SDK for Java")
                   .build();

           CreateRoleResponse response = iam.createRole(request);
           System.out.println("The ARN of the role is " +
response.role().arn());

       } catch (IamException e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
       }
       return "";
   }

   public static Object readJsonSimpleDemo(String filename) throws Exception {
```

```
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「CreateRole」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

ロールを作成します。

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
```

```
      ],
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- API の詳細については、AWS SDK for JavaScript API リファレンスの「CreateRole」を参照してください。

PHP

SDK for PHP

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
```

```
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
            ]);
        });
        return $result['Role'];
    }
```

- API の詳細については、「AWS SDK for PHP API リファレンス」の「CreateRole」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、**MyNewRole** という名前の新しいロールを作成し、**NewRoleTrustPolicy.json** ファイルにあるポリシーをそのロールにアタッチします。JSON ポリシーファイルを正常に処理するには、**-Raw** switch パラメータを使用する必要があることに注意してください。出力に表示されるポリシードキュメントは、URL でエンコードされています。この例では、**UrlDecode** .NET メソッドを使用してデコードされています。

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

出力:

```
Arn                       : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
```

```
                              %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                              %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                              %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                              %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                              %20%5D%0D%0A%7D
CreateDate                  : 4/15/2015 11:04:23 AM
Path                        : /
RoleId                      : V5PAJI2KPN4EAEXAMPLE1
RoleName                    : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「CreateRole」を参照してください。

Tools for PowerShell V5

例 1: この例では、**MyNewRole** という名前の新しいロールを作成し、**NewRoleTrustPolicy.json** ファイルにあるポリシーをそのロールにアタッチします。JSON ポリシーファイルを正常に処理するには、**-Raw** switch パラメータを使用する必要があることに注意してください。出力に表示されるポリシードキュメントは、URL でエンコードされています。この例では、**UrlDecode** .NET メソッドを使用してデコードされています。

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

出力:

```
Arn                      : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                           %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                           %20%5D%0D%0A%7D
CreateDate               : 4/15/2015 11:04:23 AM
Path                     : /
RoleId                   : V5PAJI2KPN4EAEXAMPLE1
RoleName                 : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V5)」の「CreateRole」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
```

```
    else:
        return role
```

- API の詳細については、「AWS SDK for Python (Boto3) API Reference」の「CreateRole」を参照してください。

Ruby

SDK for Ruby

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
 # Creates a role and attaches policies to it.
 #
 # @param role_name [String] The name of the role.
 # @param assume_role_policy_document [Hash] The trust relationship policy
document.
 # @param policy_arns [Array<String>] The ARNs of the policies to attach.
 # @return [String, nil] The ARN of the new role if successful, or nil if an
error occurred.
 def create_role(role_name, assume_role_policy_document, policy_arns)
   response = @iam_client.create_role(
     role_name: role_name,
     assume_role_policy_document: assume_role_policy_document.to_json
   )
   role_arn = response.role.arn

   policy_arns.each do |policy_arn|
     @iam_client.attach_role_policy(
       role_name: role_name,
       policy_arn: policy_arn
     )
   end
```

```
    role_arn
  rescue Aws::IAM::Errors::ServiceError => e
    @logger.error("Error creating role: #{e.message}")
    nil
  end
```

- API の詳細については、「AWS SDK for Ruby API リファレンス」の「CreateRole」を参照してください。

Rust

SDK for Rust

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- API の詳細については、「AWS SDK for Rust API リファレンス」の「CreateRole」を参照してください。

Swift

SDK for Swift

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import AWSIAM
import AWSS3


    public func createRole(name: String, policyDocument: String) async throws ->
 String {
        let input = CreateRoleInput(
            assumeRolePolicyDocument: policyDocument,
            roleName: name
        )
        do {
            let output = try await client.createRole(input: input)
            guard let role = output.role else {
                throw ServiceHandlerError.noSuchRole
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            print("ERROR: createRole:", dump(error))
            throw error
        }
    }
```

- API の詳細については、「AWS SDK for Swift API リファレンス」の「CreateRole」を参照してください。

を使用したカスタマーマネージド設定レコーダー AWS Config から開始する AWS CLI

まず、カスタマーマネージド設定レコーダー AWS Config を作成します。を使用してカスタマー管理設定レコーダーを作成するには AWS CLI、、put-configuration-recorderput-delivery-channel、および のコマンドを使用しますstart-configuration-recorder。

- put-configuration-recorder コマンドは、カスタマーマネージド設定レコーダーを作成します。
- put-delivery-channel コマンドは、 が S3 バケットと SNS トピックに設定情報を AWS Config 配信する配信チャネルを作成します。
- は、カスタマーマネージド設定レコーダーstart-configuration-recorderを起動します。カスタマーマネージド設定レコーダーは、指定したリソースタイプの設定変更の記録を開始します。

トピック

- 考慮事項
- ステップ 1: put-configuration-recorder を実行する
- ステップ 2: put-delivery-channel コマンドを実行する
- ステップ 3: start-configuration-recorder コマンドを実行する

考慮事項

S3 バケット、SNS トピック、IAM ロールが必要です

カスタマーマネージド設定レコーダーを作成するには、S3 バケット、SNS トピック、およびポリシーがアタッチされた IAM ロールを前提条件として作成する必要があります。の前提条件を設定するには AWS Config、「前提条件」を参照してください。

リージョンごとにアカウントごとに 1 つのカスタマーマネージド設定レコーダー

AWS アカウント カスタマー管理設定レコーダーは、 ごとに 1 つだけ持つことができます AWS リージョン。

リージョンごとにアカウントごとに 1 つの配信チャネル

配信チャネルリージョンは、それぞれ 1 AWS アカウント つのみ持つことができます AWS リージョン。

ポリシーとコンプライアンスの結果

で管理される IAM ポリシーやその他のポリシーは、 がリソースの設定変更を記録するアクセス許可を持つかどうか AWS Config に影響を与える可能性があります。 AWS Organizationsさらに、 ルールはリソースの設定を直接評価し、 ルールは評価の実行時にこれらのポリシーを考慮しません。有効なポリシーが、使用する意図と一致していることを確認してください AWS Config。

ステップ 1: put-configuration-recorder を実行する

put-configuration-recorder コマンドを使用して、カスタマーマネージド設定レコーダーを作成します。

このコマンドは、[--configuration-recorder] フィールドと [---recording-group] フィールドを使用します。

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

configuration-recorderフィールド

[configurationRecorder.json] ファイルは、name および roleArn、さらに設定レコーダーのデフォルトの記録頻度を指定します (recordingMode)。このフィールドを使用して、特定のリソースタイプの記録頻度を上書きすることもできます。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

recording-groupフィールド

recordingGroup.json ファイルは、記録するリソースタイプを指定します。

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

これらのフィールドの詳細については、「 コマンドリファレンスput-configuration-recorder」の「」を参照してください。 AWS CLI

ステップ 2: put-delivery-channel コマンドを実行する

put-delivery-channel コマンドを使用して配信チャネルを作成します。

このコマンドは --delivery-channelフィールドを使用します。

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

delivery-channelフィールド

deliveryChannel.json ファイルは以下を指定します。

- 配信チャネルnameの 。
- s3BucketName が設定スナップショット AWS Config を送信する 。
- snsTopicARN が通知 AWS Config を送信する 。
- configSnapshotDeliveryProperties は、 が設定スナップショットを AWS Config 配信する頻度と、定期的なルールの評価を呼び出す頻度を設定します。

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
```

```
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

これらのフィールドの詳細については、「 コマンドリファレンスput-delivery-channel」の「」を参照してください。 AWS CLI

ステップ 3: start-configuration-recorder コマンドを実行する

start-configuration-recorder コマンドを使用して以下を開始します AWS Config。

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

これらのフィールドの詳細については、「 コマンドリファレンスstart-configuration-recorder」の「」を参照してください。 AWS CLI

AWS Config が正常に開始されたことを確認する AWS CLI

開始したら AWS Config、 AWS CLI コマンドを使用して、 AWS Config が実行されていること、および AWS Config が設定レコーダーと配信チャネルを作成したことを確認できます。 AWS Config が設定の記録と配信チャネルへの配信を開始したことを確認することもできます。

トピック

- ステップ 1: 配信チャネルが作成されていることを確認する
- ステップ 2: 設定レコーダーが作成されていることを確認する
- ステップ 3: AWS Config が記録を開始したことを確認する

ステップ 1: 配信チャネルが作成されていることを確認する

describe-delivery-channels コマンドを使用して、Amazon S3 バケットおよび Amazon SNS トピックが設定済みであることを確認します。

`--delivery-channel-names` フィールドを使用して、配信チャネルのリストを指定できます。配信チャネルが指定されていない場合、このコマンドはアカウントに関連付けられているすべての配信チャネルの詳細を返します。

```
$ aws configservice describe-delivery-channels
```

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

ステップ 2: 設定レコーダーが作成されていることを確認する

describe-configuration-recorders コマンドを使用して、設定レコーダーが作成されていることを確認します。

arn および configuration-recorder-namesフィールドを使用して、設定レコーダーのリストを指定できます。設定レコーダーが指定されていない場合、このコマンドはアカウントに関連付けられているすべての設定レコーダーの詳細を返します。

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

ステップ 3: AWS Config が記録を開始したことを確認する

describe-configuration-recorder-status コマンドを使用して、設定レコーダーが範囲内のリソースタイプを正常に記録していることを確認します。

arn および configuration-recorder-namesフィールドを使用して、設定レコーダーのリストを指定できます。設定レコーダーが指定されていない場合、このコマンドはアカウントに関連付けられているすべての設定レコーダーの詳細を返します。

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
```

```
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

`recording` フィールドの`true`値は、設定レコーダーが設定の記録を開始したことを確認します。AWS Config は時刻を UTC で記録します。出力は Unix timestamp として表示されます。

AWS SDK AWS Config での の使用

AWS Software Development Kit (SDKsは、多くの一般的なプログラミング言語で使用できます。各 SDK には、デベロッパーが好みの言語でアプリケーションを簡単に構築できるようにする API、コード例、およびドキュメントが提供されています。

SDK ドキュメント	コード例
AWS SDK for C++	AWS SDK for C++ コード例
AWS CLI	AWS CLI コード例
AWS SDK for Go	AWS SDK for Go コード例
AWS SDK for Java	AWS SDK for Java コード例
AWS SDK for JavaScript	AWS SDK for JavaScript コード例
AWS SDK for Kotlin	AWS SDK for Kotlin コード例
AWS SDK for .NET	AWS SDK for .NET コード例
AWS SDK for PHP	AWS SDK for PHP コード例
AWS Tools for PowerShell	AWS Tools for PowerShell コード例

SDK ドキュメント	コード例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) コード例
AWS SDK for Ruby	AWS SDK for Ruby コード例
AWS SDK for Rust	AWS SDK for Rust コード例
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP コード例
AWS SDK for Swift	AWS SDK for Swift コード例

可用性の例

必要なものが見つからなかった場合。このページの下側にある [Provide feedback (フィードバックを送信)] リンクから、コードの例をリクエストしてください。

設定レコーダーの使用

設定レコーダーは、スコープ内のリソースタイプに対する設定変更を設定項目 (CIsとして保存します。

設定レコーダーには 2 つのタイプがあります。

Type	説明
カスタマーマネージド設定レコーダー	管理した設定レコーダー。スコープ内のリソースタイプはユーザーが設定します。デフォルトでは、カスタマーマネージド設定レコーダー AWS Config は、 AWS リージョン が実行されている でサポートされているすべてのリソースを記録します。
サービスにリンクされた設定レコーダー	特定の にリンクされた設定レコーダー AWS のサービス。スコープ内のリソースタイプは、リンクされたサービスによって設定されます。

トピック

- カスタマーマネージド設定レコーダーに関する考慮事項
- サービスにリンクされた設定レコーダーに関する考慮事項
- 設定レコーダーのドリフト検出
- カスタマーマネージド設定レコーダーの起動
- カスタマーマネージド設定レコーダーの停止
- カスタマーマネージド設定レコーダーの記録頻度の変更
- カスタマーマネージド設定レコーダーの名前変更
- 設定レコーダーの表示
- 設定レコーダーの削除

カスタマーマネージド設定レコーダーに関する考慮事項

リージョンごとにアカウントごとに 1 つのカスタマーマネージド設定レコーダー

カスタマーマネージド設定レコーダーは、それぞれ 1 つのみ持つことができます AWS アカウント AWS リージョン。

デフォルトでは、グローバル IAM リソースタイプを除く、サポートされているすべてのリソースタイプが記録されます。

カスタマーマネージド設定レコーダーのデフォルトは、サポートされているすべてのリソースタイプを記録することです。ただし、、`AWS::IAM::Role`、`AWS::IAM::GroupAWS::IAM::Policy`および `AWS::IAM::User` のグローバル IAM リソースタイプは除きます。記録に含めるリソースタイプまたは記録から除外するリソースタイプを指定できます。

詳細については、「を使用した AWS リソースの記録 AWS Config」を参照してください。

カスタマーマネージド設定レコーダーの使用には、サービス使用料が課金されます。

がカスタマーマネージド設定レコーダーで設定の記録 AWS Config を開始すると、サービス使用料が課金されます。

料金に関する情報については、[AWS Config の料金]を参照してください。

AWS Systems Manager を使用して組織全体でカスタマーマネージド設定レコーダーを作成する

AWS Systems Manager 高速セットアップを使用して、複数の組織単位 (OUsカスタマーマネージド設定レコーダーを作成し、 AWS ベストプラクティス AWS リージョン を使用できます。

詳細については、「Systems Manager ユーザーガイド」の「高速セットアップを使用して AWS Config 設定レコーダーを作成する」を参照してください。

> **Important**
>
> ポリシーとコンプライアンス結果
> で管理される IAM ポリシーやその他のポリシーは、 AWS Config がリソースの設定変更を記録するアクセス許可を持っているかどうかに影響を与える可能性があります。 AWS Organizationsさらに、 ルールはリソースの設定を直接評価し、 ルールは評価の実行時にこれらのポリシーを考慮しません。有効なポリシーが、使用する意図と一致していることを確認してください AWS Config。
> 設定レコーダーがオフになっている場合、削除されたリソースの古い評価結果は保持される可能性があります

カスタマーマネージド設定レコーダーがオフになっている場合、 AWS Config Config が削除など、指定したリソースの設定の変更を追跡する機能が無効になります。つまり、カスタマーマネージド設定レコーダーがオフになっていると、 は記録がオンになっていないと削除イベントをキャプチャ AWS Config できないため、削除されたリソースの評価結果が古くなる可能性があります。

サービスにリンクされた設定レコーダーに関する考慮事項

AWS Config サービスにリンクされたロールを使用する必要があります

AWS Config サービスにリンクされたロールは、サービスにリンクされた設定レコーダーに必要です。

詳細については、「AWS Config用のサービスリンクロールの使用」を参照してください。

サービスにリンクされた設定レコーダーは常に記録されます

サービスにリンクされた設定レコーダーの記録を停止または開始することはできません。記録を停止するには、サービスにリンクされた設定レコーダーを削除する必要があります。

詳細については、「設定レコーダーの削除」を参照してください。

記録スコープは、設定項目を受信するかどうかを決定します。

記録範囲は、設定レコーダーにリンクされたサービスによって設定され、配信チャネルで設定項目 (CIs) を受信するかどうかを決定します。録画スコープが内部の場合、配信チャネルで CIsを受信しません。

記録範囲によって、サービス料金が請求されるかどうかが決まります。

記録範囲は、設定レコーダーにリンクされたサービスによって設定され、範囲内の設定項目 (CIs) が無料 (INTERNAL) で記録されるか、請求コスト (PAID) に影響するかを決定します。

サポートされる サービス

サービスにリンクされた設定レコーダーは、次のサービスでサポートされています。

AWS service	サービスプリンシパル	で を使用する利点 AWS Config	詳細はこちら
Amazon CloudWatch	`observabilityadmin.amazonaws.com`	Amazon CloudWatch Observability Admin を使用して、 AWS 組織またはアカウントの CloudWatch のテレメトリ設定の状態を検出して理解できます。	詳細については、CloudWatch ユーザーガイド」の「CloudWatch テレメトリ設定の監査」を参照してください。CloudWatch
AWS Security Hub	`securityhub.amazonaws.com`	を使用して AWS Security Hub 、セキュリティ検出結果を一元管理し、 AWS アカウント全体でセキュリティ評価を実行できます。サービスにリンクされたレコーダーを使用すると、露出分析カバレッジに必要なリソース設定項目を取得するためのイベント駆動型のアプローチが可能になります。	詳細については、「 Security Hub ユーザーガイド」の「Security Hub を有効にする」を参照してください。

設定レコーダーのドリフト検出

`AWS::Config::ConfigurationRecorder` リソースタイプは、設定レコーダーの状態に対するすべての変更を追跡する設定レコーダーの設定項目 (CI) です。この CI を使用して、設定レコーダーの状態が以前の状態と異なるか、ドリフトしたかを確認できます。

例えば、この CI は、 AWS Config で追跡を有効にしたリソースタイプに更新があるかどうか、設定レコーダーを停止または起動したか、設定レコーダーを削除またはアンインストールしたかを追跡し

ます。ドリフトした設定レコーダーは、目的のリソースタイプへの変更を正確に検出していないことを示します。設定レコーダーがドリフトしていると、コンプライアンス結果が偽陰性または偽陽性になる可能性があります。

`AWS::Config::ConfigurationRecorder` リソースタイプは のシステムリソースタイプ AWS Config であり、このリソースタイプの記録は、サポートされているすべてのリージョンでデフォルトで有効になっています。`AWS::Config::ConfigurationRecorder` リソースタイプの記録は、追加料金なしでご利用いただけます。

カスタマーマネージド設定レコーダーの起動

AWS Config コンソールを使用するか、カスタマーマネージド設定レコーダー AWS CLI を起動できます。

To start the customer managed configuration recorder (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. カスタマーマネージドレコーダータブで、録画の開始を選択します。プロンプトが表示されたら、確認 を選択します。

To start the customer managed configuration recorder (CLI)

`start-configuration-recorder`コマンドを使用します。

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

カスタマーマネージド設定レコーダーの停止

> **Note**
>
> サービスにリンクされた設定レコーダーは常に記録されます
>
> サービスにリンクされた設定レコーダーは常に記録されるため、サービスにリンクされた設定レコーダーを停止することはできません。記録を停止するには、サービスにリンクされた

設定レコーダーを削除する必要があります。詳細については、「設定レコーダーの削除」を参照してください。

AWS Config コンソールを使用するか、カスタマーマネージド設定レコーダー AWS CLI を停止できます。

To stop the customer managed configuration recorder (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. カスタマーマネージドレコーダータブで、録画を停止を選択します。プロンプトが表示されたら、確認を選択します。

To stop the customer managed configuration recorder (CLI)

`stop-configuration-recorder`コマンドを使用します。

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

カスタマーマネージド設定レコーダーの記録頻度の変更

AWS Config は、継続的な記録と毎日の記録をサポートしています。

- 継続的な記録により、変更が発生するたびに設定の変更を継続的に記録できます。
- 毎日の記録では、過去 24 時間のリソースの最新の状態を表す設定項目 (CI) を受け取ることができます。これは、記録された以前の CI と異なる場合に限ります。詳細については、「Recording Frequency」を参照してください。

AWS Config コンソールを使用するか、録画頻度を AWS CLI 変更できます。

To change the recording frequency for the customer managed configuration recorder (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。

2. ナビゲーションペインで [設定] を選択します。
3. カスタマーマネージドレコーダータブで、録画の開始を選択します。
4. Recording method managed recorder で、カスタマイズ可能なオーバーライドを持つすべてのリソースタイプを選択します。
5. デフォルト設定で、記録頻度を選択します。
6. [保存] を選択します。

To change the recording frequency (CLI)

put-configuration-recorder のコマンドを使用して、設定レコーダーの記録頻度を変更します。

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

[configurationRecorder.json] ファイルは、name および roleArn、さらに設定レコーダーのデフォルトの記録頻度を指定します (recordingMode)。このフィールドを使用して、特定のリソースタイプの記録頻度をオーバーライドすることもできます。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

put-configuration-recorder コマンドは、--configuration-recorder パラメータで次のフィールドを使用します。

- name – 設定レコーダーの名前。 AWS Config は、設定レコーダーの作成時に名前「デフォルト」を自動的に割り当てます。
- roleARN – 設定レコーダーが引き受け AWS Config 、使用する IAM ロールの Amazon リソースネーム (ARN)。
- recordingMode – が設定変更を記録 AWS Config するために使用するデフォルトの記録頻度を指定します。 は継続的な記録と毎日の記録 AWS Config をサポートします。継続的な記録により、変更が発生するたびに設定の変更を継続的に記録できます。日時記録により、以前に記録された CI と異なる場合にのみ、過去 24 時間におけるリソースの最新の状態を表す設定項目 (CI) を、受け取ることができます。
  - recordingFrequency – AWS Config が設定変更を記録するために使用するデフォルトの記録頻度。

    > **Note**
    > AWS Firewall Manager は、リソースをモニタリングするために継続的な記録に依存します。Firewall Manager を使用している場合、記録頻度を連続に設定することをお勧めします。

  - recordingModeOverrides – このフィールドで、記録モードのオーバーライドを指定できます。recordingModeOverride オブジェクトの配列です。recordingModeOverrides 配列の各 recordingModeOverride オブジェクトは、次の 3 つのフィールドで構成されます。
    - description - オーバーライドに入力した説明。
    - recordingFrequency - オーバーライドで指定されたすべてのリソースタイプに適用される記録頻度。
    - resourceTypes – オーバーライド AWS Config に含めるリソースタイプを指定するカンマ区切りリスト。

> **Note**
> 必須フィールドとオプションフィールド put-configuration-recorder の recordingMode フィールドはオプションです。デフォルトでは、設定レコーダーの記録頻度は継続的な記録に設定されています。

> **Note**
>
> 制限
>
> 次のリソースタイプに日次記録はサポートされていません。
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> 現在および将来サポートされるすべてのリソースタイプを記録する (ALL_SUPPORTED_RESOURCE_TYPES) 記録方法について、これらのリソースタイプは継続的な記録に設定されます。

カスタマーマネージド設定レコーダーの名前変更

カスタマーマネージド設定レコーダーの名前 AWS CLI を変更するには、 を使用する必要があります。カスタマー管理設定レコーダーの名前を変更するには、そのレコーダーを削除し、指定した名前で新しい設定レコーダーを作成する必要があります。

を使用したカスタマーマネージド設定レコーダーの名前変更 AWS CLI

1. `describe-configuration-recorders` コマンドを使用して、現在のカスタマーマネージド設定レコーダーの名前を検索します。

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

2. `delete-configuration-recorder` コマンドを使用して、カスタマー管理の現在の設定レコーダーを削除します。

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. put-configuration-recorder コマンドを使用して、新しい名前でカスタマーマネージド設定レコーダーを作成します。

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. start-configuration-recorder コマンドを使用して記録を再開します。

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

設定レコーダーの表示

AWS Config コンソールを使用するか、設定レコーダーの詳細 AWS CLI を表示できます。

To view your configuration recorders (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. カスタマーマネージド設定レコーダーの場合、カスタマーマネージドレコーダータブで詳細を表示できます。
4. サービスにリンクされた設定レコーダーの場合は、サービスにリンクされたレコーダータブでサービスにリンクされた設定レコーダーを選択し、表示を選択します。

To view your configuration recorders (CLI)

describe-configuration-recorders コマンドを使用して、設定レコーダーの詳細を表示します。

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
```

```
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

describe-configuration-recorder-status コマンドを使用して、設定レコーダーの現在のステータスを表示します。

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

これらのコマンドの両方で、 フィールドarnと configuration-recorder-namesフィールドを使用して設定レコーダーのリストを指定できます。サービスにリンクされた設定レコーダーの場合、 service-principalフィールドを使用して設定レコーダーを指定できます。

設定レコーダーが指定されていない場合、このコマンドはアカウントに関連付けられているすべての設定レコーダーの詳細を返します。

設定レコーダーの削除

カスタマーマネージド設定レコーダーを削除するには AWS CLI 、 を使用する必要があります。AWS Config コンソールまたは を使用して AWS CLI 、サービスにリンクされた設定レコーダーを削除できます。

To delete the customer managed configuration recorder (CLI)

delete-configuration-recorderコマンドを使用します。

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To delete a service-linked configuration recorder (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. サービスにリンクされたレコーダータブで、サービスにリンクされたレコーダータブでサービスにリンクされた設定レコーダーを選択し、削除を選択します。プロンプトが表示されたら、[削除] を選択します。

To delete a service-linked configuration recorder (CLI)

`delete-service-linked-configuration-recorder`コマンドを使用します。

このコマンドは `--service-principal`フィールドを使用します。

```
$ aws configservice delete-service-linked-configuration-recorder --service-principal
 "The service principal of the AWS ##### for the service-linked configuration
 recorder that you want to delete"
```

配信チャネルの使用

は、 AWS リソースに発生した変更 AWS Config を継続的に記録し、配信チャネルを介して通知と更新された設定状態を送信します。配信チャネルを管理して、 が設定更新 AWS Config を送信する場所を制御できます。

トピック

- 考慮事項
- 用語
- 設定項目のコンポーネント
- 配信チャネルの表示
- 配信チャネルの更新
- 配信チャネルの名前変更
- Amazon S3 バケットへの設定スナップショットの配信
- 配信ステータスを確認する
- Amazon S3 バケットの設定スナップショットの表示
- からの設定スナップショットの例 AWS Config
- Amazon SNS トピック AWS Config に送信する通知

考慮事項

各アカウントのリージョンごとに 1 つの配信チャネル

AWS リージョンごとにリージョンごとに 1 つの配信チャネルのみを持つことができ AWS アカウント、配信チャネルを使用する必要があります AWS Config。

オーバーサイズの設定項目通知には、簡単な概要が含まれます

がリソースの設定変更 AWS Config を検出し、通知が Amazon SNS で許可されている最大サイズを超えると、通知には設定項目の概要が含まれます。通知の全詳細は、`s3BucketLocation` フィールドで指定した Amazon S3 バケット内に表示されています。詳細については、[サイズが大きすぎる設定項目の変更に関する通知の例] を参照してください。

AWS Config が使用する Amazon S3 バケットの AWS KMS 暗号化をサポート AWS Config

AWS Key Management Service （ AWS KMS) キーまたはエイリアス Amazon リソースネーム (ARN) を指定して、Amazon Simple Storage Service (Amazon S3) バケットに配信されるデータを暗号化できます。デフォルトでは、 は設定履歴とスナップショットファイルを Amazon S3 バケットに AWS Config 配信し、S3 AES-256 サーバー側の暗号化 SSE-S3 を使用して保管中のデータを暗号化します。ただし、 AWS Config に KMS キーまたはエイリアス ARN を指定した場合、 は AES-256 暗号化の代わりにその KMS キー AWS Config を使用します。

AWS Config は、オブジェクトロックが有効になっていてデフォルトの保持が有効になっている Amazon S3 バケットへの配信チャネルをサポートしていません。詳細については、[How S3 Object Lock works (S3 オブジェクトロックの使い方)] を参照してください。

用語

設定項目は、アカウントに存在するサポートされている AWS リソースのさまざまな属性のpoint-in-timeビューを表します。設定項目のコンポーネントには、メタデータ、属性、関係、現在の設定、関連イベントが含まれます。 は、記録するリソースタイプへの変更を検出するたびに設定項目 AWS Config を作成します。たとえば、 AWS Config が Amazon S3 バケットを記録している場合、 はバケットが作成、更新、または削除されるたびに設定項目 AWS Config を作成します。 AWS Config に を選択して、設定した記録頻度で設定項目を作成することもできます。

設定履歴は、特定期間の特定リソースに関する設定項目のコレクションです。設定履歴から、リソースの最初の作成日、先月の設定内容、昨日午前 9 時に行われた設定変更などを確認できます。設定履歴は複数の形式で利用できます。 は、記録される各リソースタイプの設定履歴ファイルを、指定した Amazon S3 バケット AWS Config に自動的に配信します。 AWS Config コンソールで特定のリソースを選択し、タイムラインを使用してそのリソースの以前のすべての設定項目に移動できます。また、リソースの設定項目の履歴には API からアクセスすることもできます。

設定スナップショットは、アカウント内のサポートされているリソースに関する設定項目のコレクションです。設定スナップショットは、記録対象のリソースとその設定の全体像を示します。設定スナップショットは設定を検証するのに役立ちます。例えば、設定スナップショットを定期的に調べて、設定が間違っているリソースや不要と思われるリソースを見つけることができます。設定スナップショットは複数の形式で利用できます。設定スナップショットは、ユーザーが指定した Amazon Simple Storage Service (Amazon S3) バケットに配信できます。さらに、 AWS Config コンソールでポイントインタイムを選択し、リソース間の関係を使用して設定項目のスナップショット内を移動できます。

設定ストリームは、記録するリソースのすべての設定項目の自動更新リスト AWS Config です。リソースが作成、変更、または削除されるたびに、 AWS Config は設定項目を作成して設定ストリームに追加します。設定のストリーミングでは、ユーザーが選択した Amazon Simple Notification

Service (Amazon SNS) トピックを使用します。設定ストリームは、潜在的な問題を特定したり、特定のリソースが変更された場合に通知を生成したり、 AWS リソースの設定を反映する必要がある外部システムを更新したりできるように、設定変更が発生したときに監視するのに役立ちます。

設定項目のコンポーネント

設定項目は、アカウントに存在するサポートされている AWS リソースのさまざまな属性のpoint-in-timeビューを表します。設定項目のコンポーネントには、メタデータ、属性、関係、現在の設定、関連イベントが含まれます。 は、記録するリソースタイプへの変更を検出するたびに設定項目 AWS Config を作成します。たとえば、 AWS Config が Amazon S3 バケットを記録している場合、 はバケットが作成、更新、または削除されるたびに設定項目 AWS Config を作成します。 AWS Config でを選択して、設定した記録頻度で設定項目を作成することもできます。

設定項目は以下のコンポーネントで構成されます。

コンポーネント	説明	を含む
メタデータ	この設定項目に関する情報	• バージョン ID • 設定項目がキャプチャされた時刻 • 設定項目が正常にキャプチャされたかどうかを示す、設定項目のステータス • リソースの設定項目の順序を示す状態 ID
属性	リソース属性	• Resource ID (リソース ID) • このリソースのキーバリュータグのリスト • リソースタイプ (「でサポートされているリソースタイプ AWS Config」を参照) • Amazon リソースネーム (ARN) • このリソースが含まれているアベイラビリティーゾーン (該当する場合) • リソースが作成された時刻
関係	このリソースと、アカウントに関連付けられた他のリソースとの関係	関係の説明 (Amazon EBS ボリューム `vol-1234567` は Amazon EC2 インスタ

コンポーネント	説明	を含む
		ンス `i-a1b2c3d4` にアタッチされているなど)
現行の設定	リソースの Describe または List の API 呼び出しを通じて返される情報	例えば、`DescribeVolumes` API はボリュームに関する以下の情報を返します。 • ボリュームがあるアベイラビリティーゾーン • ボリュームがアタッチされた時刻 • アタッチ先の EC2 インスタンスの ID • ボリュームの現在のステータス • DeleteOnTermination フラグの状態 • ボリュームのアタッチ先のデバイス • ボリュームのタイプ (`gp2`, `io1`,、`standard` など)

メモ

1. 設定項目の関係には、ネットワークフローやデータフローの依存関係は含まれません。アプリケーションアーキテクチャを反映するように設定項目をカスタマイズすることはできません。
2. バージョン 1.3 では、relatedEvents フィールドは空です。リソースのイベントを取得する方法については、AWS CloudTrail API リファレンスの LookupEvents API を参照してください。
3. バージョン 1.3 では、configurationItemMD5Hash フィールドは空です。configurationStateId フィールドを使用すると、最新の設定項目があることを確認できます。
4. リソースタイプがタグ付けをサポートしていない場合、または describe API レスポンスにタグ情報が含まれていない場合、 AWS Config はそのリソースタイプの設定項目 (CIs) にタグデータをキャプチャしません。 AWS Config は引き続きこれらのリソースを記録します。ただし、タグデータに依存する機能は機能しません。これは、タグデータに依存するタグベースのフィルタリング、グループ化、またはコンプライアンス評価に影響します。

配信チャネルの表示

配信チャネルの詳細を表示するには AWS CLI 、 を使用する必要があります。

次のサンプルコードは、DescribeDeliveryChannels を使用する方法を説明しています。

CLI

AWS CLI

配信チャネルの詳細を取得するには

次のコマンドは、配信チャネルに関する詳細を返します。

```
aws configservice describe-delivery-channels
```

出力:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeDeliveryChannels」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、リージョンの配信チャネルを取得し、詳細を表示します。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

出力:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
```

```
default config-bucket-NA my          TwentyFour_Hours
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V4)」のDescribeDeliveryChannels」を参照してください。

Tools for PowerShell V5

例 1: この例では、リージョンの配信チャネルを取得し、詳細を表示します。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

出力:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のDescribeDeliveryChannels」を参照してください。

配信チャネルの更新

配信チャネルを更新する場合は、以下のオプションを設定できます。

- が設定スナップショットと設定履歴ファイル AWS Config を送信する Amazon S3 バケット。
- が Amazon S3 バケットに設定スナップショット AWS Config を配信する頻度。
- が設定変更に関する通知 AWS Config を送信する Amazon SNS トピック。

配信チャネルを更新するには (コンソール)

AWS Config コンソールを使用して、配信チャネルの Amazon S3 バケットと Amazon SNS トピックを設定できます。これらの設定を管理する手順については、[コンソール AWS Config で をセットアップする] を参照してください。

コンソールには、配信チャネルの名前変更、設定スナップショットの頻度の設定、または配信チャネルの削除のオプションはありません。これらのタスクを実行するには、、 AWS Config API AWS CLI、またはいずれかの AWS SDKsを使用する必要があります。

配信チャネル (AWS SDKsを更新するには

次のサンプルコードは、PutDeliveryChannel を使用する方法を説明しています。

CLI

AWS CLI

配信チャネルを作成するには

次のコマンドは、配信チャネルの設定を JSON コードとして提供します。

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

deliveryChannel.json ファイルは、配信チャネルの属性を指定します。

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

この例では以下の属性を設定します。

name - 配信チャネルの名前です。デフォルトでは、 AWS Config は新しい配信チャネルdefaultに名前を割り当てます。 put-delivery-channel コマンドを使用して配信チャネル名を更新することはできません。名前を変更する手順については、「配信チャネルの名前変更」を参照してください。s3BucketName- Config が設定スナップショットと設定履歴ファイルを配信する Amazon S3 AWS バケットの名前。別の AWS アカウントに属するバケットを指定する場合、そのバケットには Config AWS にアクセス許可を付与するポリシーが必要です。詳細については、Amazon S3 バケットのアクセス許可を参照してください。

snsTopicARN - Config が設定変更に関する通知を送信する Amazon SNS トピックの Amazon リソースネーム (ARN)。別のアカウントからトピックを選択した場合、トピックには Config AWS にアクセス許可を付与するポリシーが必要です。 AWS 詳細については、「Permissions for the Amazon SNS Topic」を参照してください。

configSnapshotDeliveryProperties - deliveryFrequency 属性が含まれます。これは、Config AWS が設定スナップショットを配信する頻度と、定期的な Config ルールの評価を呼び出す頻度を設定します。

コマンドが成功すると、 AWS Config は出力を返しません。配信チャネルの設定を確認するには、describe-delivery-channels コマンドを実行します。

- API の詳細については、「AWS CLI コマンドリファレンス」の「PutDeliveryChannel」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、既存の配信チャネルの deliveryFrequency プロパティを変更します。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V4)」のPutDeliveryChannel」を参照してください。

Tools for PowerShell V5

例 1: この例では、既存の配信チャネルの deliveryFrequency プロパティを変更します。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のPutDeliveryChannel」を参照してください。

設定を記録して配信チャネルに配信するためのアクセス許可を `describe-delivery-channels` に付与するポリシーを新しいロールにアタッチする必要があります。

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
```

```
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

次のサンプルコードは、DescribeDeliveryChannels を使用する方法を説明しています。

CLI

AWS CLI

配信チャネルの詳細を取得するには

次のコマンドは、配信チャネルに関する詳細を返します。

```
aws configservice describe-delivery-channels
```

出力:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeDeliveryChannels」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、リージョンの配信チャネルを取得し、詳細を表示します。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

出力:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V4)」のDescribeDeliveryChannels」を参照してください。

Tools for PowerShell V5

例 1: この例では、リージョンの配信チャネルを取得し、詳細を表示します。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

出力:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V5)」のDescribeDeliveryChannels」を参照してください。

配信チャネルの名前変更

配信チャネルの名前を変更するには、まず現在の配信チャネルを削除し、次に指定した名前で作り直す必要があります。配信チャネルを削除する前に、一時的に設定レコーダーを停止する必要があります。 AWS Config コンソールには、配信チャネルを削除するオプションはありません。CLI、 AWS Config API、またはいずれかの AWS SDKs AWS を使用する必要があります。

を使用した配信チャネルの名前変更 AWS CLI

1. `stop-configuration-recorder`コマンドを使用して設定レコーダーを停止します。

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. describe-delivery-channelsコマンドを使用して配信チャネルの属性を書き留めます。

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. delete-delivery-channelコマンドを使用して配信チャネルを削除します。

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. put-delivery-channelコマンドを使用して、新しい名前で配信チャネルを作成します。

```
$ aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

deliveryChannel.json ファイルは、配信チャネルの属性を指定します。

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. `start-configuration-recorder` コマンドを使用して記録を再開します。

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Amazon S3 バケットへの設定スナップショットの配信

設定スナップショットは、アカウント内のサポートされているリソースに関する設定項目のコレクションです。設定スナップショットは、記録対象のリソースとその設定の全体像を示します。設定スナップショットは設定を検証するのに役立ちます。例えば、設定スナップショットを定期的に調べて、設定が間違っているリソースや不要と思われるリソースを見つけることができます。設定スナップショットは複数の形式で利用できます。設定スナップショットは、ユーザーが指定した Amazon Simple Storage Service (Amazon S3) バケットに配信できます。さらに、 AWS Config コンソールでポイントインタイムを選択し、リソース間の関係を使用して設定項目のスナップショット内を移動できます。

設定スナップショットを配信する

AWS Config DeliverConfigSnapshot アクションを呼び出すか、 AWS CLI `deliver-config-snapshot` コマンドを実行すると、 は設定スナップショットを生成します。 は、 を有効にしたときに指定した Amazon S3 バケットに設定スナップショット AWS Config を保存します AWS Config。

配信チャネルを設定 AWS Config したときに によって割り当てられた名前を指定して、 `deliver-config-snapshot` コマンドを入力します。次に例を示します。

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

配信ステータスを確認する

`describe-delivery-channel-status` コマンドを入力して、 AWS Config が指定された配信チャネルへの設定の配信を開始したことを確認します。

```
aws configservice describe-delivery-channel-status
```

レスポンスには、 AWS Config が設定をバケットとトピックに配信するために使用する 3 つの配信形式すべてのステータスが一覧表示されます。

```
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
    ]
}
```

`configSnapshotDeliveryInfo` で `lastSuccessfulTime` フィールドを表示します。時刻は、前回に設定スナップショットの配信をリクエストした時刻と一致する必要があります。

> **Note**
>
> AWS Config は UTC 形式 (協定世界時) を使用して時刻を記録します。

Amazon S3 バケットの設定スナップショットの表示

設定スナップショットは、アカウント内のサポートされているリソースに関する設定項目のコレクションです。設定スナップショットは、記録対象のリソースとその設定の全体像を示します。設定スナップショットは設定を検証するのに役立ちます。例えば、設定スナップショットを定期的に調べて、設定が間違っているリソースや不要と思われるリソースを見つけることができます。設定スナップショットは複数の形式で利用できます。設定スナップショットは、ユーザーが指定した Amazon Simple Storage Service (Amazon S3) バケットに配信できます。さらに、 AWS Config コンソールでポイントインタイムを選択し、リソース間の関係を使用して設定項目のスナップショット内を移動できます。

設定スナップショットの表示

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. Amazon S3 コンソールの [すべてのバケット] リストで、Amazon S3 バケットの名前を選択します。
3. バケット内のネストされたフォルダをすべて確認して、コマンドから返された ID と一致するスナップショット ID の `ConfigSnapshot` オブジェクトを表示します。オブジェクトをダウンロードして開き、設定スナップショットを表示します。S3 バケットには、 という名前の空のファイルも含まれています`ConfigWritabilityCheckFile`。 はこのファイル AWS Config を作成して、サービスが S3 バケットに正常に書き込めることを確認します。

からの設定スナップショットの例 AWS Config

設定スナップショットに AWS Config が含まれる情報の例を次に示します。スナップショットは、の現在のリージョンで記録 AWS Config しているリソースの設定と AWS アカウント、これらのリソース間の関係を記述します。

> **Note**
> 設定スナップショットには、サポートされていないリソースタイプとリソース ID への参照を含めることができます。

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
```

```
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
```

```
            "configurationItemVersion": "1.0",
            "resourceId": "i-344c463d",
            "accountId": "12345678910",
            "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
            "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
            "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
```

```
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
                ],
```

```
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
```

```
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```


次のステップでは、設定スナップショットが配信チャネルに正常に配信されたことを確認します。

Amazon SNS トピック AWS Config に送信する通知

> **Note**
>
> AWS Config が Amazon SNS トピックに通知を送信する前に、まず設定レコーダーと配信チャネルを設定する必要があります。詳細については、「設定レコーダーの管理」および「配信チャネルの管理」を参照してください。

設定の変更と通知 AWS Config を Amazon SNS トピックにストリーミングするように を設定できます。例えば、リソースの更新時に E メールアドレスに通知が送信されれば、変更を確認できます。

が リソースに対してカスタムルールまたはマネージドルール AWS Config を評価するときに通知を受け取ることもできます。詳細については、「ログインとモニタリング AWS Config」を参照してください。

AWS Config は、次のイベントの通知を送信します。

- リソースの設定項目の変更。
- リソースの設定履歴がアカウントに配信された。
- 記録対象のリソースの設定スナップショットがアカウントで起動および配信された。
- リソースのコンプライアンス状態とリソースがルールに準拠するかどうか。
- リソースに対してルールの評価が開始された。
- AWS Config は通知をアカウントに配信できませんでした。

トピック

- 設定項目の変更の通知例
- 設定履歴の配信通知の例
- 設定スナップショットの配信開始の通知例
- 設定スナップショットの配信通知の例
- コンプライアンス変更の通知の例
- ルールの評価開始の通知例
- サイズが大きすぎる設定項目の変更の通知例
- 配信失敗の通知の例

設定項目の変更の通知例

AWS Config は Amazon SNS を使用してサブスクリプションエンドポイントに通知を配信します。これらの通知は、設定スナップショットと設定履歴の配信ステータスを提供し、記録された AWS リソースの設定が変更されたときに が AWS Config 作成する各設定項目を提供します。 AWS Config は、リソースがルールに準拠しているかどうかを示す通知も送信します。通知を E メールで送信することを選択した場合は、E メールクライアントアプリケーションで E メールの件名とメッセージ本文にフィルタを適用できます。

次の例は、Amazon Elastic Block Store ボリューム `vol-ce676ccc` が `i-344c463d` を ID とするインスタンスにアタッチされていることを AWS Config が検出した場合に生成される Amazon SNS 通知のペイロードを示しています。通知には、リソースの設定品目の変更が含まれています。

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "awsAccountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
```

```
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```

関係を持つリソースの設定項目

リソースが他のリソースに関連付けられている場合、そのリソースの変更に伴って複数の設定項目が生じることがあります。次の例は、 がリレーションシップを持つリソースの設定項目 AWS Config を作成する方法を示しています。

1. `i-007d374c8912e3e90` を ID とする EC2 インスタンスがあり、このインスタンスは Amazon EC2 セキュリティグループの `sg-c8b141b4` に関連付けられています。
2. EC2 インスタンスを更新して、セキュリティグループを別のセキュリティグループ `sg-3f1fef43` に変更します。
3. EC2 インスタンスは別のリソースに関連付けられているため、 は次の例のような複数の設定項目 AWS Config を作成します。

この通知には、セキュリティグループの置換に伴う EC2 インスタンスの設定項目の変更が含まれています。

```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
```

```
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
```

```
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
```

```
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
                        "groupId": "sg-c8b141b4"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
                {
                    "resourceId": "eni-fde9493f",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::NetworkInterface",
                    "name": "Contains NetworkInterface"
                },
                {
                    "resourceId": "sg-3f1fef43",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::SecurityGroup",
                    "name": "Is associated with SecurityGroup"
                },
                {
                    "resourceId": "subnet-2372be7b",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Subnet",
                    "name": "Is contained in Subnet"
                },
```

```
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::VPC",
                    "name": "Is contained in Vpc"
                }
            ],
            "configuration": {
                "instanceId": "i-007d374c8912e3e90",
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "ec2-micro",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t2.micro",
                "launchTime": "2017-01-09T20:13:28.000Z",
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
```

```
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
```

```
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
```

```
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


次の通知には、インスタンスに関連付けられている EC2 セキュリティグループ sg-3f1fef43 の設定項目の変更が含まれています。


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
```

```
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
```

```
}
```

Amazon SNS **ConfigurationItemChangeNotification** 通知の **configurationItemDiff** フィールドについて

AWS Config は、リソースの設定が変更 (create/update/delete) されるたびに設定項目を作成します。が記録 AWS Config できるサポートされているリソースタイプのリストについては、「」を参照してください[でサポートされているリソースタイプ AWS Config](#)。 AWS Config はAmazon SNS を使用して、変更が発生したときに通知を配信します。Amazon SNS 通知ペイロードには、特定の AWS リージョンのリソースの変更を追跡するのに役立つフィールドが含まれています。

`ConfigurationItemChangeNotification` 通知を受け取る理由を理解するには、`configurationItemDiff` の詳細を確認します。フィールドは変更タイプによって異なり、UPDATE-UPDATE、UPDATE-CREATE、および DELETE-DELETE など、組み合わせはさまざまです。一般的な組み合わせは次のとおりです。

UPDATE-CREATE と UPDATE-UPDATE

次の例には、リソースの直接関係とリソース設定の変更が含まれています。`configurationItemDiff` の詳細は、次の情報を公開します。

実行されたアクション: アカウントに存在する管理ポリシーが AWS Identity and Access Management (IAM) ロールにアタッチされました。

実行された基本的なオペレーション: UPDATE (アカウントのリソースタイプ `AWS::IAM::Policy` の関連付けの数を更新)。

変更タイプの組み合わせ:

1. リソースダイレクトの関係は、更新-作成を変更します。IAM ポリシーと IAM ロールの間に新しいアタッチメントまたはアソシエーションが作成されました。
2. リソース設定は、UPDATE-CREATE を変更します。ポリシーが IAM ロールにアタッチされたとき、IAM ポリシーの関連付けの数は 2 から 3 に増加しました。

UPDATE-CREATE と UPDATE-UPDATE `configurationItemDiff` 通知の例:

```
{
    "configurationItemDiff": {
```

```
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

UPDATE-DELETE

次の例には、リソースの直接関係とリソース設定の変更が含まれています。`configurationItemDiff` の詳細は、次の情報を公開します。

実行されたアクション: アカウントに存在するマネージドポリシーが、IAM ユーザーからデタッチされました。

実行された基本的なオペレーション: UPDATE (リソースタイプ `AWS::IAM::User` に関連付けられたアクセス許可ポリシーの更新)。

変更タイプの組み合わせ: リソース直接関係の変更 UPDATE-DELETE。アカウントの IAM ユーザーと IAM ポリシー間の関連付けが削除されました。

UPDATE-DELETE `configurationItemDiff` 通知の例:

JSON

```
{
  "configurationItemDiff": {
    "changedProperties": {
```

```
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                        >>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
  }
}
```

DELETE-DELETE

次の例には、リソースの直接関係とリソース設定の変更が含まれています。`configurationItemDiff` の詳細は、次の情報を公開します。

実行されたアクション: アカウントに存在する IAM ロールが削除されました。

実行された基本的なオペレーション: DELETE (リソースタイプ `AWS::IAM::Role` のリソースが削除されました)。

変更タイプの組み合わせ: リソース直接関係の変更とリソース設定の変更 DELETE-DELETE。IAM ロールを削除により、IAM ポリシーと IAM ロールとの関連付けも削除されました。

DELETE-DELETE `configurationItemDiff` 通知の例:

JSON


```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
          "name": "Is attached to CustomerManagedPolicy"
        },
        "updatedValue": null,
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/
AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
          "roleLastUsed": null
        },
        "updatedValue": null,
        "changeType": "DELETE"
      }
    },
```

```
    "changeType": "DELETE"
}
```

設定履歴の配信通知の例

設定履歴は、特定期間の特定リソースタイプに関する設定項目のコレクションです。以下は、CloudTrail 証跡リソースの設定履歴がアカウントに配信されたときに が AWS Config 送信する通知の例です。

```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

設定スナップショットの配信開始の通知例

が アカウントの設定スナップショットの配信 AWS Config を開始したときに AWS Config が送信する通知の例を次に示します。

```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


設定スナップショットの配信通知の例

設定スナップショットは、アカウント内のすべての記録されたリソースとその設定に関する設定項目のコレクションです。以下は、アカウントの設定スナップショットが配信されたときに が AWS Config 送信する通知の例です。


```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
```

```
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


コンプライアンス変更の通知の例

がカスタムルールまたはマネージドルールに対してリソース AWS Config を評価すると、 はリソースがルールに準拠しているかどうかを示す通知 AWS Config を送信します。

次の例は、CloudTrail 証跡リソースが `cloudtrail-enabled` マネージドルールに準拠していることを示す通知です。


```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
```

```
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
```

```
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

例: 設定項目の変更 | Amazon EventBridge

```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
```

```
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
```

```
    }
  }
}
```

ルールの評価開始の通知例

AWS Config は、カスタムルールまたはマネージドルールをリソースに対して評価し始めると、通知を送信します。が `iam-password-policy`マネージドルールの評価 AWS Config を開始するときの通知の例を次に示します。

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

サイズが大きすぎる設定項目の変更の通知例

がリソースの設定変更 AWS Config を検出すると、設定項目 (CI) 通知が送信されます。通知が Amazon Simple Notification Service (Amazon SNS) の最大許容サイズを超えている場合、通知には設定項目の概要が含まれます。

通知の全詳細は、`s3BucketLocation` フィールドで指定した Amazon S3 バケット内に表示されています。

次の通知例は、Amazon EC2 インスタンスの CI を示しています。通知には、変更の概要と Amazon S3 バケット内の通知の参照先が含まれています。

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
```

```
        "s3BucketLocation": "amzn-s3-demo-bucket/AWSLogs/123456789012/
Config/us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

オーバーサイズの設定項目にアクセスする方法

設定項目がオーバーサイズの場合、概要のみが Amazon SNS に送信されます。完全な設定項目 (CI) は Amazon S3 に保存されます。

次のコード例は、完全な CI にアクセスする方法を示しています。

```
import boto3
import json

def handle_oversized_configuration_item(event):
    """
    Example of handling an oversized configuration item notification

    When a configuration item is oversized:
    1. AWS Config sends a summary notification through SNS
    2. The complete configuration item is stored in S3
    3. Use get_resource_config_history API to retrieve the complete configuration
    """

    # Extract information from the summary notification
    if event['messageType'] == 'OversizedConfigurationItemChangeNotification':
        summary = event['configurationItemSummary']
        resource_type = summary['resourceType']
        resource_id = summary['resourceId']

        # Initialize AWS Config client
        config_client = boto3.client('config')

        # Retrieve the complete configuration item
```

```
        response = config_client.get_resource_config_history(
            resourceType=resource_type,
            resourceId=resource_id
        )

        if response['configurationItems']:
            config_item = response['configurationItems'][0]

            # For EC2 instances, the configuration contains instance details
            configuration = json.loads(config_item['configuration'])
            print(f"Instance Configuration: {configuration}")

            # Handle supplementary configuration if present
            if 'supplementaryConfiguration' in config_item:
                for key, value in config_item['supplementaryConfiguration'].items():
                    if isinstance(value, str):
                        config_item['supplementaryConfiguration'][key] =
 json.loads(value)
                print(f"Supplementary Configuration:
 {config_item['supplementaryConfiguration']}")

            return config_item

        # If needed, you can also access the complete notification from S3
        s3_location = event['s3DeliverySummary']['s3BucketLocation']
        print(f"Complete notification available in S3: {s3_location}")

    return None
```

仕組み

1. 関数は、 AWS Config 通知を含むイベントパラメータを受け入れます。
2. メッセージタイプがオーバーサイズの設定通知であるかどうかをチェックします。
3. 関数は、概要からリソースタイプと ID を抽出します。
4. AWS Config クライアントを使用して、完全な設定履歴を取得します。
5. 関数は、メイン設定と補足設定の両方を処理します。
6. 必要に応じて、指定された S3 の場所から完全な通知にアクセスできます。

配信失敗の通知の例

AWS Config が設定スナップショットまたはオーバーサイズの設定項目変更通知を Amazon AWS Config S3 バケットに配信できない場合、 は配信失敗通知を送信します。 Amazon S3 有効な Amazon S3 バケットを指定したことを確認してください。

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
```

```
    "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
    "recordVersion": "1.0"
  }
```

AWS Config ダッシュボードの表示

ダッシュボードを使用して、リソース、ルール、コンフォーマンスパック、およびそれらのコンプライアンス状態の概要を確認し、Amazon CloudWatch の AWS Config 使用状況と成功のメトリクスを視覚化します。このページでは、 AWS アカウント内の上位リソース、 のコンプライアンスレベルが最も低いコンフォーマンスパック AWS アカウント、 の非準拠ルールまたはリソース AWS アカウント、 AWS Config 使用を促進しているトラフィック、ワークフローで発生した成功と失敗の主要なメトリクスをすばやく特定できます。

AWS Config ダッシュボードを使用するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. 左のナビゲーションペインの [VPC Dashboard] (VPC ダッシュボード) を選択します。

目次

- コンプライアンスおよびリソースインベントリ
- AWS Config 使用状況と成功のメトリクス

コンプライアンスおよびリソースインベントリ

セットアップ後、 は指定されたリソースの記録とルールに対する評価 AWS Config を開始します。がリソース、ルール、コンフォーマンスパック、およびそれらのコンプライアンス状態を表示する AWS Config までに数分かかる場合があります。

コンプライアンススコア別のコンフォーマンスパック

コンプライアンススコア別のコンフォーマンスパックでは、コンプライアンススコアの低い順にコンフォーマンスパックが 10 個まで表示されます。コンプライアンススコアは、コンフォーマンスパック内の可能なルールとリソースの組み合わせの合計数に対する、コンフォーマンスパック内のコンプライアンスルールとリソースの組み合わせの数の割合です。

このメトリクスにより、コンフォーマンスパックのコンプライアンス状態の概要が表示され、コンフォーマンスパックのコンプライアンスレベルを特定、調査、把握するために使用できます。このコンプライアンススコアを使用して修復の進行状況を追跡し、さまざまな要件セット間で比

較を実行して、特定の変更またはデプロイがコンフォーマンスパックに与える影響を確認できます。

デプロイステータス、コンプライアンススコア、コンプライアンススコアのタイムライン、およびコンフォーマンスパックのルールを詳細ビューで表示するには、[コンフォーマンスパック] でコンフォーマンスパックの名前を選択します。

コンプライアンス状況

コンプライアンスステータスは、準拠ルール、非準拠ルール、および非準拠リソースの数を表示します。リソースは、関連付けられたルールの評価に基づいて、準拠または非準拠です。リソースがルールの仕様に従わない場合、リソースとルールには非準拠のフラグが付けられます。

非準拠ルールとリソースのリストを表示するには、[Noncompliant rule(s)] (非準拠ルール) または [Noncompliant resource(s)] (非準拠のリソース) を選択します。

非準拠リソースによるルール

[Rules by noncompliant resource count] (非準拠リソース数によるルール) は、上位の非準拠ルールをリソース数の降順で表示します。ルールを選択して、その特定のルールのスコープ内の詳細、パラメータ、およびリソースを表示します。

非準拠ルールの包括的なリストについては、[View all noncompliant rules] (非準拠ルールの表示) を選択します。

リソースインベントリ

リソースインベントリには、 AWS Config が記録しているリソースの総数を、リソースの数と の各リソースタイプの数で降順に表示します AWS アカウント。リソースタイプのすべてのリソースを開くには、そのリソースタイプを選択して、その [Resources inventory] (リソースインベントリ) ページに移動します。

ドロップダウンリストを使用して、表示するリソースの合計を指定できます。デフォルトでは、すべてのリソースを表示するように設定されていますが、 AWS リソース、サードパーティーリソース、またはカスタムリソースに変更できます。

> **Note**
>
> Config ルールを使用して AWS リソース設定を評価するメッセージは、次の理由で ダッシュボードに表示されることがあります。

- の AWS Config ルールを設定していません AWS アカウント。ルールの追加 を選択してルール ページに移動できます。
- AWS Config は、引き続き ルールに照らしてリソースを評価しています。ページを更新して、最新の評価結果を表示します。
- AWS Config はリソースをルールに対して評価し、範囲内のリソースが見つかりませんでした。設定ページで記録 AWS Config する のリソースを指定できます。詳細については、「を使用した AWS リソースの記録 AWS Config」を参照してください。

AWS Config 使用状況と成功のメトリクス

AWS Config コンソールで Amazon CloudWatch ダッシュボードを使用して、 AWS Config 使用状況と成功のメトリクスを視覚化できます。

各ダッシュボードから、次の操作を実行できます。

- ダッシュボードの時間範囲を調整し、過去 3 時間、1 日、1 週間のデータを表示します。
- [カスタム] を選択して、カスタム時間範囲を入力します。過去に指定した時間の [相対] 時間か、2 つの日付の間の [絶対] 時間範囲のいずれかを選択します。
- 時間形式を変更して、ダッシュボードのデータを UTC (協定世界時) またはローカルタイムゾーン (使用しているデバイスのオペレーティングシステムでローカルタイムゾーンとして指定されている時間帯) で表示することができます。
- ダッシュボードのデータの更新する頻度を指定したり、自動更新をオフにしたりするには、[Refresh icon] (更新アイコン) の隣にある Drop arrow (ドロップ矢印) を使用します。[Off] (オフ)、[10 Seconds] (10 秒)、[1 Minute] (1 分)、[2 Minutes] (2 分)、[5 Minutes] (5 分)、または [15 Minutes] (15 分) を選択して更新間隔を変更します。
- その他のオプション (縦の省略記号メニュー) を選択して、現在 AWS Config Dashboard で表示している AWS Config 使用状況メトリクスまたは AWS Config 成功メトリクスを CloudWatch コンソールに追加します。これにより、CloudWatch コンソールに新しいタブが開き、現在の AWS Config 使用状況メトリクスまたは AWS Config 成功メトリクスからコピーされた情報を使用して CloudWatch で新しいカスタムダッシュボードを作成できます。

CloudWatch でこれらのメトリクスの追加の分析を実行する場合は、CloudWatch コンソールの左側のナビゲーションペインで [Metrics] (メトリクス) を選択し、[AWS/Config] (AWS/ 設定) を選択します。CloudWatch コンソールから実行できる操作の詳細については、CloudWatch ユーザーガイドの

「Amazon CloudWatch ダッシュボードの使用」と「Amazon CloudWatch メトリクスの使用」を参照してください。

AWS Config 使用状況メトリクス

メトリクス	説明	単位	
Configuration Items Recorded	各リソースタイプまたはすべてのリソースタイプについて記録された設定項目の数。設定項目は、サポートされている AWS リソースのさまざまな属性のpoint-in-timeビューを表します。設定項目または対応するリソースタイプの詳細については、「設定項目と「対応するリソースタイプ」を参照してください。	カウント	

ドロップダウンリストを使用して、表示するリソースタイプを選択できます。デフォルトでは、すべてのリソースタイプを表示するように設定されています。

AWS Config 成功メトリクス

メトリクス	説明	単位	
Change Notifications Delivery Failed	配信チャネルの Amazon SNS トピックへの変更通知配信の失敗回数。変更通知は、AWS リソースの設定状態の変更を通知します。ConfigStreamDeliveryInfo API を使用して、変更通知の最後に試行された配信の `lastErrorCode` または `lastErrorMessage` を取得できます。詳細については、「配信チャネルの管理」を参照してください。	カウント	
Config History Export Failed	Amazon S3 バケットへの設定履歴のエクスポートに失敗した回数。設定履歴は、特定期間の特定リソースに関する設定項目のコレクションです。設定履歴の詳細については、「設定履歴」を参照してください。	カウント	

メトリクス	説明	単位	
`Configuration Recorder Insufficient Permissions Failure`	アカウント内のすべての設定レコーダーの IAM ロールポリシーが原因で失敗したアクセス許可の試行回数。アクセス許可 AWS リージョン が不十分です。設定レコーダーは、範囲内のリソースタイプに対する の変更を検出します。設定レコーダーが AWS リソース設定を記録するには、必要な IAM アクセス許可が必要です。詳細については、「設定詳細を取得するための IAM ロールポリシー」を参照してください。	カウント	
`Config Snapshot Export Failed`	Amazon S3 バケットへの設定スナップショットのエクスポートに失敗した回数。設定スナップショットは、アカウント内のサポートされているリソースに関する設定項目のコレクションです。設定スナップショットの詳細については、「設定スナップショット」を参照してください。	Count (カウント)	

を使用した AWS リソース設定の管理と表示 AWS Config

AWS Config では、 AWS リソースの設定を評価、監査、評価できます。

AWS リソースは、、 AWS Command Line Interface (CLI) AWS Management Console、 AWS SDKs。 AWS リソースの例としては AWS 、Amazon EC2 インスタンス、セキュリティグループ、Amazon VPCs、Amazon Elastic Block Store などがあります。 は、リソース ID や Amazon リソースネーム (ARN) などの一意の識別子を使用して各リソース AWS Config を参照します。

一般的ユースケースには以下のようなものが含まれます。

- クラウド管理者: リソース設定を追跡および管理して、コンプライアンスの確保、問題のトラブルシューティング、 AWS 環境の理解の維持に役立てることができます。
- セキュリティアナリスト: リソース設定を必要な状態と照らし合わせて評価し、脆弱性の特定とセキュリティ体制の評価を支援できます。
- コンプライアンスオフィサー: リソース設定を継続的に監査およびモニタリングして、組織のポリシーと業界標準への準拠を確保できます。

トピック

- でサポートされているリソースタイプ AWS Config
- 利用可能なリージョン別リソースカバレッジ
- を使用した AWS リソースの記録 AWS Config
- を使用したサードパーティーリソース AWS Config の による設定の記録 AWS CLI
- を使用したマネージドインスタンスのソフトウェア設定の記録 AWS Config
- によって検出されたリソースの検索 AWS Config
- を使用した AWS リソースのコンプライアンス情報と評価結果の表示 AWS Config
- を使用した AWS リソースのコンプライアンス履歴の表示 AWS Config
- AWS リソースのコンプライアンス履歴のクエリ
- AWS Config リソースのタグ付け

でサポートされているリソースタイプ AWS Config

> **Important**
>
> このページは、毎月初めに更新されます。

AWS Config では、次の AWS リソースタイプとリソース関係がサポートされています。

- リソースタイプの詳細については、 AWS CloudFormation ユーザーガイドのリソースおよびAWS プロパティタイプのリファレンスのリファレンス情報 (構文、プロパティ、戻り値など) を参照してください。
- AWS Config 記録のために、一部の AWS リージョンではこれらのリソースタイプのサブセットがサポートされています。どのリソースタイプがどのリージョンでサポートされているかについては、「利用可能なリージョン別リソースカバレッジ」を参照してください。
- の高度なクエリは、これらのリソースタイプのサブセット AWS Config をサポートします。サポートされているリソースタイプのリストについては、「Supported Resource Types for Advanced Queries」を参照してください。
- のプロアクティブ評価は、これらのリソースタイプのサブセット AWS Config をサポートします。サポートされているリソースタイプのリストについては、「プロアクティブ評価用にサポートされているリソースタイプ」を参照してください。
- 定期的なルールは設定項目 (CIs) に依存しないため、定期的なルールは設定レコーダーを有効にせずに実行されます。変更によってトリガーされるルールと定期的なルールの違いの詳細については、AWS Config 「ルールの評価モードとトリガータイプ」を参照してください。

  つまり、ルールページを表示すると、リストされている CI やサポートされているリソースはありません。リソース ID を選択すると、 というエラーが表示されます`The provided resource ID and resource type cannot be found`。これは想定される動作です。

> **Note**
>
> リソースタイプのリージョンの可用性
> が追跡 AWS Config するリソースタイプを指定する前に、Resource Coverage by Region Availability をチェックして、リソースタイプがセットアップした AWS リージョンでサポートされているかどうかを確認します AWS Config。リソースタイプが少なくとも 1 つのリージョン AWS Config で でサポートされている場合は、指定したリソースタイプがセットアッ

プしたリージョンでサポートされていない場合でも AWS Config、 でサポートされているすべての AWS リージョンでそのリソースタイプの記録を有効にできます AWS Config。
リソースタイプのタグ付けのサポート
リソースタイプがタグ付けをサポートしていない場合、または describe API レスポンスにタグ情報が含まれていない場合、そのリソースタイプの設定項目 (CIs) AWS Config にタグデータはキャプチャされません。 AWS Config は引き続きこれらのリソースを記録します。ただし、タグデータに依存する機能は機能しません。これは、タグデータに依存するタグベースのフィルタリング、グループ化、またはコンプライアンス評価に影響します。

Amazon AppStream

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon AppStream	`AWS::AppStream::DirectoryConfig`	NA	該当なし
	`AWS::AppStream::Application`	該当なし	該当なし
	`AWS::AppStream::Stack`	該当なし	該当なし
	`AWS::AppStream::Fleet`	該当なし	NA

Amazon AppFlow

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon AppFlow	`AWS::AppFlow::Flow`	NA	NA

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon AppIntegrations	`AWS::AppIntegrations::EventIntegration`	NA	該当なし
	`AWS::AppIntegrations::Application`	該当なし	NA

Amazon API Gateway

AWS サービス	リソースタイプの値	関係	関連リソース
API Gateway	`AWS::ApiGateway::Stage`	is contained in	ApiGateway Rest Api
		is associated with	WAFRegional WebACL
	`AWS::ApiGateway::RestApi`	contains	ApiGateway Stage
API Gateway V2	`AWS::ApiGatewayV2::Stage`	is contained in	ApiGatewayV2 Api
	`AWS::ApiGatewayV2::Api`	contains	ApiGatewayV2 Stage

と Amazon API Gateway AWS Config の統合方法の詳細については、「[による API Gateway API 設定のモニタリング AWS Config](#)」を参照してください。

Amazon Athena

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Athena	`AWS::Athena::WorkGroup`	NA	該当なし
	`AWS::Athena::DataCatalog`	該当なし	該当なし
	`AWS::Athena::PreparedStatement`	該当なし	NA

Amazon Bedrock

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Bedrock	`AWS::Bedrock::Guardrail`	NA	該当なし
	`AWS::Bedrock::KnowledgeBase`	該当なし	NA

Amazon CloudFront

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon CloudFront	`AWS::CloudFront::Distribution`	is associated with	AWS WAF WebACL
			ACM 証明書
			S3 バケット

AWS サービス	リソースタイプの値	関係	関連リソース
			IAM サーバー証明書
	`AWS::CloudFront::PublicKey`	NA	NA
	`AWS::CloudFront::StreamingDistribution`	is associated with	AWS WAF WebACL
			ACM 証明書
			S3 バケット
			IAM サーバー証明書

Amazon CloudWatch

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	NA	該当なし
	`AWS::CloudWatch::MetricStream`	該当なし	NA
Amazon CloudWatch Logs	`AWS::Logs::Destination`	NA	NA
Amazon CloudWatch RUM	`AWS::RUM::AppMonitor`	NA	NA
Amazon CloudWatch Evidently	`AWS::Evidently::Project`	NA	該当なし
	`AWS::Evidently::Launch`	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::Evidently::Segment`	該当なし	NA

Amazon CodeGuru

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon CodeGuru Reviewer	`AWS::CodeGuruReviewer::RepositoryAssociation`	NA	NA
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	NA	NA

Amazon Cognito

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Cognito	`AWS::Cognito::UserPool`	NA	該当なし
	`AWS::Cognito::UserPoolClient`	該当なし	該当なし
	`AWS::Cognito::UserPoolGroup`	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::Cognito::IdentityPool`	該当なし	NA

Amazon Connect

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Connect	`AWS::Connect::PhoneNumber`	NA	該当なし
	`AWS::Connect::QuickConnect`	該当なし	該当なし
	`AWS::Connect::Instance`	該当なし	該当なし
	`AWS::Connect::Rule`	該当なし	該当なし
	`AWS::Connect::User`	該当なし	NA
Amazon Connect Customer Profiles	`AWS::CustomerProfiles::Domain`	NA	該当なし
	`AWS::CustomerProfiles::ObjectType`	該当なし	NA

Amazon Detective

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Detective	`AWS::Detective::Graph`	NA	NA

Amazon DynamoDB

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon DynamoDB	`AWS::DynamoDB::Table`	NA	NA

Amazon Elastic Compute Cloud

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Elastic Compute Cloud	`AWS::EC2::Host` *	contains	EC2 インスタンス
	`AWS::EC2::EIP`	is attached to	EC2 インスタンス
			ネットワークインターフェイス
	`AWS::EC2::Instance`	contains	EC2 ネットワークインターフェイス
		is associated with	EC2 セキュリティグループ
		is attached to	Amazon EBS ボリューム
			EC2 Elastic IP (EIP)

AWS サービス	リソースタイプの値	関係	関連リソース
		is contained in	EC2 専有ホスト
			ルートテーブル
			サブネット
			仮想プライベートクラウド (VPC)
	`AWS::EC2::NetworkInterface`	is associated with	EC2 セキュリティグループ
		is attached to	EC2 Elastic IP (EIP)
			EC2 インスタンス
		is contained in	ルートテーブル
			サブネット
			仮想プライベートクラウド (VPC)
	`AWS::EC2::SecurityGroup` *	is associated with	EC2 インスタンス
			EC2 ネットワークインターフェイス
			仮想プライベートクラウド (VPC)
	`AWS::EC2::NatGateway`	is contained in	Virtual Private Cloud (VPC)
		is contained in	サブネット

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::EC2::EgressOnlyInternetGateway	is attached to	仮想プライベートクラウド (VPC)
	AWS::EC2::EC2Fleet	NA	該当なし
	AWS::EC2::SpotFleet	該当なし	該当なし
	AWS::EC2::PrefixList	該当なし	該当なし
	AWS::EC2::FlowLog	該当なし	該当なし
	AWS::EC2::TransitGateway	該当なし	該当なし
	AWS::EC2::TransitGatewayAttachment	該当なし	該当なし
	AWS::EC2::TransitGatewayRouteTable	該当なし	NA
	AWS::EC2::VPCEndpoint	is contained in	Virtual Private Cloud (VPC)
		is attached to	ネットワークインターフェイス

AWS サービス	リソースタイプの値	関係	関連リソース
		is contained in	サブネット
		is contained in	ルートテーブル
	`AWS::EC2::VPCEndpointService`	is associated with	ElasticLoadBalancingV2 LoadBalancer
	`AWS::EC2::VPCPeeringConnection`	is associated with	仮想プライベートクラウド (VPC)
	`AWS::EC2::RegisteredHAInstance`	is associated with	EC2 インスタンス
	`AWS::EC2::SubnetRouteTableAssociation`	NA	該当なし
	`AWS::EC2::LaunchTemplate`	該当なし	該当なし
	`AWS::EC2::NetworkInsightsAccessScopeAnalysis`	該当なし	該当なし
	`AWS::EC2::TrafficMirrorTarget`	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::EC2::TrafficMirrorSession	該当なし	該当なし
	AWS::EC2::DHCPOptions	該当なし	該当なし
	AWS::EC2::IPAM	該当なし	該当なし
	AWS::EC2::IPAMResourceDiscovery	該当なし	該当なし
	AWS::EC2::IPAMResourceDiscoveryAssociation	該当なし	該当なし
	AWS::EC2::NetworkInsightsPath	該当なし	該当なし
	AWS::EC2::TrafficMirrorFilter	該当なし	該当なし
	AWS::EC2::CapacityReservation	該当なし	該当なし
	AWS::EC2::ClientVpnEndpoint	該当なし	NA

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::EC2::Customer Gateway`	is attached to	VPN 接続
	`AWS::EC2::Internet Gateway`	is attached to	仮想プライベートクラウド (VPC)
	`AWS::EC2::NetworkAcl`	NA	NA
	`AWS::EC2::RouteTable`	contains	EC2 インスタンス
			EC2 ネットワークインターフェイス
			サブネット
			VPN ゲートウェイ
		is contained in	仮想プライベートクラウド (VPC)
	`AWS::EC2::Subnet`	contains	EC2 インスタンス
			EC2 ネットワークインターフェイス
		is attached to	ネットワーク ACL
		is contained in	ルートテーブル
			仮想プライベートクラウド (VPC)
	`AWS::EC2::VPC`	contains	EC2 インスタンス

AWS サービス	リソースタイプの値	関係	関連リソース
			EC2 ネットワークインターフェイス
			ネットワーク ACL
			ルートテーブル
			サブネット
		is associated with	セキュリティグループ
		is attached to	インターネットゲートウェイ
			VPN ゲートウェイ
	`AWS::EC2::VPNConnection`	is attached to	カスタマーゲートウェイ
			VPN ゲートウェイ
	`AWS::EC2::VPNConnectionRoute`	NA	NA
	`AWS::EC2::VPNGateway`	is attached to	仮想プライベートクラウド (VPC)
			VPN 接続
		is contained in	ルートテーブル
	`AWS::EC2::IPAMScope`	NA	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::EC2::CarrierGateway	該当なし	該当なし
	AWS::EC2::TransitGatewayConnect	該当なし	該当なし
	AWS::EC2::IPAMPool	該当なし	該当なし
	AWS::EC2::TransitGatewayMulticastDomain	該当なし	該当なし
	AWS::EC2::NetworkInsightsAccessScope	該当なし	該当なし
	AWS::EC2::NetworkInsightsAnalysis	該当なし	該当なし
	AWS::EC2::VPCBlockPublicAccessOptions	該当なし	該当なし
	AWS::EC2::VPCBlockPublicAccessExclusion	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::EC2::EIPAssociation`	該当なし	該当なし
	`AWS::EC2::InstanceConnectEndpoint`	該当なし	該当なし
	`AWS::EC2::SnapshotBlockPublicAccess`	該当なし	該当なし
	`AWS::EC2::VPCEndpointConnectionNotification`	該当なし	NA
Amazon Elastic Block Store	`AWS::EC2::Volume`	is attached to	EC2 インスタンス
EC2 イメージビルダー	`AWS::ImageBuilder::ImagePipeline`	NA	該当なし
	`AWS::ImageBuilder::DistributionConfiguration`	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::ImageBuilder::ContainerRecipe`	該当なし	該当なし
	`AWS::ImageBuilder::InfrastructureConfiguration`	該当なし	該当なし
	`AWS::ImageBuilder::ImageRecipe`	該当なし	NA

*AWS Config 専有ホストと、専有ホストで起動したインスタンスの設定の詳細を記録します。その結果、サーバーにバインドされたソフトウェアライセンスへの準拠を報告するときに、 をデータソース AWS Config として使用できます。例えば、インスタンスの設定履歴を参照して、それが基づいている Amazon マシンイメージ (AMI) を判断できます。次に、ホストの設定履歴でソケット数やコア数などの詳細を参照し、ホストが AMI のライセンス要件に準拠していることを確認できます。詳細については、「Amazon EC2 ユーザーガイド」の「AWS Configで設定変更を追跡する」を参照してください。

*EC2 SecurityGroup プロパティ定義には IP CIDR ブロックが含まれており、これらは内部的に IP 範囲に変換され、特定の IP 範囲を検索しようとしたときに予期しない結果が返されることがあります。特定の IP 範囲を検索するための回避策については、「高度なクエリの制限」を参照してください。

Amazon Elastic Container Registry

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Elastic Container Registry	`AWS::ECR::Repository`	NA	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::ECR::Registry Policy`	該当なし	該当なし
	`AWS::ECR::PullThroughCacheRule`	該当なし	NA
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	NA	NA

Amazon Elastic Container Service

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Elastic Container Service	`AWS::ECS::Cluster`	NA	該当なし
	`AWS::ECS::TaskDefinition`	該当なし	該当なし
	`AWS::ECS::Service` *	該当なし	該当なし
	`AWS::ECS::TaskSet`	該当なし	該当なし
	`AWS::ECS::CapacityProvider`	該当なし	NA

* このサービスは現在、新しい Amazon リソースネーム (ARN) 形式のみをサポートします。詳細については、ECS デベロッパーガイドの Amazon リソースネーム (ARN) と ID を参照してください。

旧 (サポートされていません): `arn:aws:ecs:region:aws_account_id:service/service-name`

新 (サポートされています): `arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

Amazon Elastic File System

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Elastic File System	`AWS::EFS::FileSystem`	NA	該当なし
	`AWS::EFS::AccessPoint`	該当なし	NA

アマゾン エラスティックKubernetesサービス

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Elastic Kubernetes Service	`AWS::EKS::Cluster`	NA	該当なし
	`AWS::EKS::FargateProfile`	該当なし	該当なし
	`AWS::EKS::IdentityProviderConfig`	該当なし	該当なし
	`AWS::EKS::Addon`	該当なし	NA

Amazon EMR

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon EMR	`AWS::EMR::Security Configuration`	NA	NA

Amazon EventBridge

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon EventBridge	`AWS::Events::EventBus`	NA	該当なし
	`AWS::Events::ApiDestination`	該当なし	該当なし
	`AWS::Events::Archive`	該当なし	該当なし
	`AWS::Events::Endpoint`	該当なし	該当なし
	`AWS::Events::Connection`	該当なし	該当なし
	`AWS::Events::Rule`	該当なし	NA
Amazon EventBridge スキーマ	`AWS::EventSchemas::Registry Policy`	NA	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::EventSchemas::Discoverer	該当なし	該当なし
	AWS::EventSchemas::Schema	該当なし	該当なし
	AWS::EventSchemas::Registry	該当なし	NA

Amazon Forecast

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Forecast	AWS::Forecast::Dataset	NA	該当なし
	AWS::Forecast::DatasetGroup	該当なし	NA

Amazon Fraud Detector

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Fraud Detector	AWS::FraudDetector::Label	NA	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::FraudDetector::EntityType	該当なし	該当なし
	AWS::FraudDetector::Variable	該当なし	該当なし
	AWS::FraudDetector::Outcome	該当なし	NA

Amazon GuardDuty

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon GuardDuty	AWS::GuardDuty::Detector	NA	該当なし
	AWS::GuardDuty::ThreatIntelSet	該当なし	該当なし
	AWS::GuardDuty::IPSet	該当なし	該当なし
	AWS::GuardDuty::Filter	該当なし	NA

Amazon Inspector

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Inspector	`AWS::InspectorV2::Filter`	NA	該当なし
	`AWS::InspectorV2::Activation`	該当なし	NA

Amazon Interactive Video Service

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Interactive Video Service	`AWS::IVS::Channel`	NA	該当なし
	`AWS::IVS::RecordingConfiguration`	該当なし	該当なし
	`AWS::IVS::PlaybackKeyPair`	該当なし	NA

Amazon Keyspaces (Apache Cassandra 向け)

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Keyspaces (Apache Cassandra 向け)	`AWS::Cassandra::Keyspace`	NA	NA

Amazon OpenSearch Service

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon OpenSearch Service (レガシー Elasticsearch)	`AWS::Elasticsearch::Domain`	is associated with	KMS キー
			EC2 セキュリティグループ
			EC2 サブネット
			仮想プライベートクラウド (VPC)
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`	NA	NA
Amazon OpenSearch Serverless	`AWS::OpenSearchServerless::VpcEndpoint`	NA	該当なし
	`AWS::OpenSearchServerless::Collection`	該当なし	NA

> **Amazon OpenSearch Service 名称変更**
>
> 2021 年 9 月 8 日に、Amazon Elasticsearch Service の名称が Amazon OpenSearch Service に変更されました。OpenSearch Service は、OpenSearch だけでなく、従来の Elasticsearch もサポートします。詳細については、「Amazon OpenSearch Service - 変更の概要」を参照してください。
> 1 つ以上のドメインを OpenSearch にアップグレードしても、既存の`AWS::Elasticsearch::Domain`リソースタイプ`AWS::OpenSearch::Domain`で数週間のデータが表示されることがあります。

Amazon Personalize

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Personalize	`AWS::Personalize::Dataset`	NA	該当なし
	`AWS::Personalize::Schema`	該当なし	該当なし
	`AWS::Personalize::Solution`	該当なし	該当なし
	`AWS::Personalize::DatasetGroup`	該当なし	NA

Amazon Pinpoint

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Pinpoint	`AWS::Pinpoint::ApplicationSettings`	NA	該当なし
	`AWS::Pinpoint::Segment`	該当なし	該当なし
	`AWS::Pinpoint::App`	該当なし	該当なし
	`AWS::Pinpoint::Campaign`	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::Pinpoint::InAppTemplate`	該当なし	該当なし
	`AWS::Pinpoint::EmailChannel`	該当なし	該当なし
	`AWS::Pinpoint::EmailTemplate`	該当なし	該当なし
	`AWS::Pinpoint::EventStream`	該当なし	NA

Amazon Quantum Ledger Database (Amazon QLDB)

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon QLDB	`AWS::QLDB::Ledger`	NA	NA

Amazon Kendra

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Kendra	`AWS::Kendra::Index`	NA	NA

Amazon Kinesis

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Kinesis	`AWS::Kinesis::Stream`	NA	該当なし
	`AWS::Kinesis::StreamConsumer`	該当なし	NA
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	NA	NA
Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`	NA	NA
Kinesis ビデオストリーム	`AWS::KinesisVideo::SignalingChannel`	NA	該当なし
	`AWS::KinesisVideo::Stream`	該当なし	NA

Amazon Lex

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Lex	`AWS::Lex::BotAlias`	NA	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::Lex::Bot`	該当なし	NA

Amazon Lightsail

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Lightsail	`AWS::Lightsail::Disk`	NA	該当なし
	`AWS::Lightsail::Certificate`	該当なし	該当なし
	`AWS::Lightsail::Bucket`	該当なし	該当なし
	`AWS::Lightsail::StaticIp`	該当なし	NA

Amazon Lookout for Metrics

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Lookout for Metrics	`AWS::LookoutMetrics::Alert`	NA	NA

Amazon Lookout for Vision

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Lookout for Vision	`AWS::LookoutVision::Project`	NA	NA

Amazon Macie

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Macie	`AWS::Macie::Session`	NA	NA

Amazon Managed Grafana

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Managed Grafana	`AWS::Grafana::Workspace`	NA	NA

Amazon Managed Service for Prometheus

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Managed Service for Prometheus	`AWS::APS::RuleGroupsNamespace`	NA	NA

Amazon MemoryDB

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon MemoryDB	`AWS::MemoryDB::SubnetGroup`	NA	NA

Amazon MQ

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon MQ	`AWS::AmazonMQ::Broker`	NA	NA

Amazon Managed Streaming for Apache Kafka

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Managed Streaming for Apache Kafka	`AWS::MSK::Cluster`	NA	該当なし
	`AWS::MSK::Configuration`	該当なし	該当なし
	`AWS::MSK::BatchScramSecret`	該当なし	該当なし
	`AWS::MSK::ClusterPolicy`	該当なし	該当なし
	`AWS::MSK::VpcConnection`	該当なし	NA

AWS サービス	リソースタイプの値	関係	関連リソース
Apache Kafka Connect 向け Amazon Managed Streaming	`AWS::KafkaConnect::Connector`	NA	NA

Amazon QuickSight

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon QuickSight	`AWS::QuickSight::DataSource`	NA	該当なし
	`AWS::QuickSight::Template`	該当なし	該当なし
	`AWS::QuickSight::Theme`	該当なし	NA

Amazon Redshift

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Redshift	`AWS::Redshift::Cluster`	is associated with	クラスターパラメータグループ
			クラスターセキュリティグループ
			クラスターサブネットグループ
			セキュリティグループ

AWS サービス	リソースタイプの値	関係	関連リソース
			仮想プライベートクラウド (VPC)
	`AWS::Redshift::ClusterParameterGroup`	NA	該当なし
	`AWS::Redshift::ClusterSecurityGroup`	該当なし	該当なし
	`AWS::Redshift::ScheduledAction`	該当なし	NA
	`AWS::Redshift::ClusterSnapshot`	is associated with	クラスター
			仮想プライベートクラウド (VPC)
	`AWS::Redshift::ClusterSubnetGroup`	is associated with	サブネット
			仮想プライベートクラウド (VPC)
	`AWS::Redshift::EventSubscription`	NA	該当なし
	`AWS::Redshift::EndpointAccess`	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::Redshift::EndpointAuthorization`	該当なし	NA

Amazon Relational Database Service

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Relational Database Service	`AWS::RDS::DBCluster`	contains	RDS DB インスタンス
		is associated with	RDS DB サブネットグループ
			EC2 セキュリティグループ
	`AWS::RDS::DBClusterSnapshot`	is associated with	RDS DB クラスター
			仮想プライベートクラウド (VPC)
	`AWS::RDS::DBInstance`	is associated with	EC2 セキュリティグループ
			RDS DB セキュリティグループ
			RDS DB サブネットグループ
	`AWS::RDS::DBSecurityGroup`	is associated with	EC2 セキュリティグループ

AWS サービス	リソースタイプの値	関係	関連リソース
			仮想プライベートクラウド (VPC)
	`AWS::RDS::DBSnapshot`	is associated with	仮想プライベートクラウド (VPC)
	`AWS::RDS::DBSubnetGroup`	is associated with	EC2 セキュリティグループ
			仮想プライベートクラウド (VPC)
	`AWS::RDS::EventSubscription`	NA	該当なし
	`AWS::RDS::GlobalCluster`	該当なし	該当なし
	`AWS::RDS::Integration`	該当なし	該当なし
	`AWS::RDS::OptionGroup`	該当なし	NA

Amazon Route 53

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Route 53	`AWS::Route53::HostedZone`	NA	該当なし
	`AWS::Route53::HealthCheck`	該当なし	NA

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Route 53 プロファイル	`AWS::Route53Profiles::Profile`	NA	該当なし
Amazon Route 53 Resolver	`AWS::Route53Resolver::ResolverEndpoint`	該当なし	該当なし
	`AWS::Route53Resolver::ResolverRule`	該当なし	該当なし
	`AWS::Route53Resolver::ResolverRuleAssociation`	該当なし	該当なし
	`AWS::Route53Resolver::FirewallDomainList`	該当なし	該当なし
	`AWS::Route53Resolver::FirewallRuleGroupAssociation`	該当なし	該当なし
	`AWS::Route53Resolver::ResolverQueryLoggingConfig`	該当なし	該当なし
	`AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation`	該当なし	該当なし
	`AWS::Route53Resolver::FirewallRuleGroup`	該当なし	NA

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Application Recovery Controller (ARC)	AWS::Route53RecoveryReadiness::Cell	NA	該当なし
	AWS::Route53RecoveryReadiness::ReadinessCheck	該当なし	該当なし
	AWS::Route53RecoveryReadiness::RecoveryGroup	該当なし	該当なし
	AWS::Route53RecoveryControl::Cluster	該当なし	該当なし
	AWS::Route53RecoveryControl::ControlPanel	該当なし	該当なし
	AWS::Route53RecoveryControl::RoutingControl	該当なし	該当なし
	AWS::Route53RecoveryControl::SafetyRule	該当なし	該当なし
	AWS::Route53RecoveryReadiness::ResourceSet	該当なし	NA

Amazon SageMaker AI

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon SageMaker AI	AWS::SageMaker::CodeRepository	NA	該当なし
	AWS::SageMaker::Domain	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::SageMaker::AppImageConfig	該当なし	該当なし
	AWS::SageMaker::Image	該当なし	該当なし
	AWS::SageMaker::Model	該当なし	該当なし
	AWS::SageMaker::NotebookInstance	該当なし	該当なし
	AWS::SageMaker::NotebookInstanceLifecycleConfig	該当なし	該当なし
	AWS::SageMaker::EndpointConfig	該当なし	該当なし
	AWS::SageMaker::Workteam	該当なし	該当なし
	AWS::SageMaker::FeatureGroup	該当なし	該当なし
	AWS::SageMaker::InferenceExperiment	該当なし	NA

Amazon Simple Email Service

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Simple Email Service	`AWS::SES::ConfigurationSet`	NA	該当なし
	`AWS::SES::ContactList`	該当なし	該当なし
	`AWS::SES::Template`	該当なし	該当なし
	`AWS::SES::ReceiptFilter`	該当なし	該当なし
	`AWS::SES::ReceiptRuleSet`	該当なし	NA

Amazon Simple Notification Service

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Simple Notification Service	`AWS::SNS::Topic`	NA	NA

Amazon Simple Queue Service

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Simple Queue Service	`AWS::SQS::Queue`	NA	NA

Amazon Simple Storage Service

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon Simple Storage Service	`AWS::S3::Bucket` *	NA	該当なし
	`AWS::S3::AccountPublicAccessBlock`	該当なし	該当なし
	`AWS::S3::MultiRegionAccessPoint`	該当なし	該当なし
	`AWS::S3::StorageLens`	該当なし	該当なし
	`AWS::S3::AccessPoint`	該当なし	該当なし
	`AWS::S3::StorageLensGroup`	該当なし	該当なし
	`AWS::S3Tables::TableBucket`	該当なし	NA
Amazon S3 Express One Zone	`AWS::S3Express::DirectoryBucket`	NA	該当なし
	`AWS::S3Express::BucketPolicy`	該当なし	NA

*S3 バケットを記録する AWS Config ように を設定していて、設定変更通知を受信していない場合は、S3 バケットポリシーに必要なアクセス許可があることを確認してください。詳細については、「S3 バケット記録のアクセス許可の管理」を参照してください。

Amazon S3 バケットの属性

AWS Config は、Amazon S3 バケットリソースタイプの次の属性も記録します。

属性	説明
AccelerateConfiguration	クライアントとバケット間でデータの長距離転送を加速化。
BucketAcl	バケットとオブジェクトへのアクセスを管理するためのアクセスコントロールリスト。
BucketPolicy	バケットへのアクセス許可を定義するポリシー。
CrossOriginConfiguration	バケットへのクロスオリジンリクエストを許可。
LifecycleConfiguration	バケット内のオブジェクトのライフサイクルを定義するルール。
LoggingConfiguration	バケットへのアクセスのリクエストを追跡するためのログ記録。
NotificationConfiguration	指定したバケットイベントに関するアラートの送信やワークフローのトリガーに使用されるイベント通知。
ReplicationConfiguration	異なる AWS リージョンのバケット間でオブジェクトを自動的に非同期コピー。
RequestPaymentConfiguration	リクエスタ支払いの有効化。
TaggingConfiguration	分類のためにバケットに追加されるタグ。タグ付けを使用して請求を追跡することもできます。
WebsiteConfiguration	バケットの静的ウェブサイトホスティングの有効化。
VersioningConfiguration	バケット内のオブジェクトに対するバージョニングの有効化。

属性の詳細については、「Amazon Simple Storage Service ユーザーガイド」中の「バケット設定オプション」を参照してください。

Amazon WorkSpaces

AWS サービス	リソースタイプの値	関係	関連リソース
Amazon WorkSpaces	`AWS::WorkSpaces::ConnectionAlias`	NA	該当なし
	`AWS::WorkSpaces::Workspace`	該当なし	NA

AWS Amplify

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Amplify	`AWS::Amplify::App`	NA	該当なし
	`AWS::Amplify::Branch`	該当なし	NA

AWS AppConfig

AWS サービス	リソースタイプの値	関係	関連リソース
AWS AppConfig	`AWS::AppConfig::Application`	NA	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::AppConfig::Environment	該当なし	該当なし
	AWS::AppConfig::ConfigurationProfile	該当なし	該当なし
	AWS::AppConfig::DeploymentStrategy	該当なし	該当なし
	AWS::AppConfig::HostedConfigurationVersion	該当なし	該当なし
	AWS::AppConfig::ExtensionAssociation	該当なし	NA

AWS App Runner

AWS サービス	リソースタイプの値	関係	関連リソース
AWS App Runner	AWS::AppRunner::VpcConnector	NA	該当なし
	AWS::AppRunner::Service	該当なし	NA

AWS App Mesh

AWS サービス	リソースタイプの値	関係	関連リソース
AWS App Mesh	`AWS::AppMesh::VirtualNode`	NA	該当なし
	`AWS::AppMesh::VirtualService`	該当なし	該当なし
	`AWS::AppMesh::VirtualGateway`	該当なし	該当なし
	`AWS::AppMesh::VirtualRouter`	該当なし	該当なし
	`AWS::AppMesh::Route`	該当なし	該当なし
	`AWS::AppMesh::GatewayRoute`	該当なし	該当なし
	`AWS::AppMesh::Mesh`	該当なし	NA

AWS AppSync

AWS サービス	リソースタイプの値	関係	関連リソース
AWS AppSync	`AWS::AppSync::GraphQLApi`	NA	NA

AWS Audit Manager

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Audit Manager	`AWS::AuditManager::Assessment`	NA	NA

AWS Auto Scaling

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	contains	Amazon EC2 インスタンス
		is associated with	Classic Load Balancer
			Auto Scaling 起動設定
			サブネット
	`AWS::AutoScaling::LaunchConfiguration`	is associated with	Amazon EC2 セキュリティグループ
	`AWS::AutoScaling::ScalingPolicy`	is associated with	Auto Scaling グループ
			アラーム
	`AWS::AutoScaling::ScheduledAction`	is associated with	Auto Scaling グループ

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::AutoScaling::WarmPool`	NA	NA

AWS Backup

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Backup	`AWS::Backup::BackupPlan`	NA	NA*
	`AWS::Backup::BackupSelection`	NA	該当なし
	`AWS::Backup::BackupVault`	NA	NA*
	`AWS::Backup::RecoveryPoint`	NA	該当なし
	`AWS::Backup::ReportPlan`	該当なし	NA
AWS バックアップゲートウェイ	`AWS::BackupGateway::Hypervisor`	NA	NA

の AWS Backup 仕組みにより、これらのリソースタイプの一部は、この表の他の AWS Backup リソースタイプに関連しています。

`AWS::Backup::BackupPlan` は、バックアッププランに多数の選択肢がある`AWS::Backup::BackupSelection`場所に関連し、 AWS Backup ボールトに複数の復旧ポイントがある`AWS::Backup::RecoveryPoint`場所に`AWS::Backup::BackupVault`関連します。

詳細については、Backup プランを使用したバックアップの管理および Backup ボールトに関する各種操作を参照してください。

AWS Batch

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Batch	`AWS::Batch::JobQueue`	NA	該当なし
	`AWS::Batch::ComputeEnvironment`	該当なし	該当なし
	`AWS::Batch::SchedulingPolicy`	該当なし	NA

AWS Billing and Cost Management

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Billing and Cost Management	`AWS::BCMDataExports::Export`	NA	NA

AWS Budgets

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Budgets	`AWS::Budgets::BudgetsAction`	NA	NA

AWS Certificate Manager

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Certificate Manager	`AWS::ACM::Certificate`	NA	NA

AWS CloudFormation

AWS サービス	リソースタイプの値	関係	関連リソース
AWS CloudFormation	`AWS::CloudFormation::GuardHook`	NA	NA
	`AWS::CloudFormation::Stack` *	contains	サポートされている AWS リソースタイプ

*AWS Config AWS CloudFormation スタックの設定変更と stacks でサポートされているリソースタイプを記録します。まだサポートされていないスタックのリソースタイプの設定変更は記録 AWS Config されません。サポートされていないリソースタイプは、スタックの設定項目の補助的な設定セクションに表示されます。

AWS CloudTrail

AWS サービス	リソースタイプの値	関係	関連リソース
AWS CloudTrail	`AWS::CloudTrail::Trail`	NA	NA

AWS Cloud9

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Cloud9	`AWS::Cloud9::EnvironmentEC2`	NA	NA

> **AWS Cloud9 新規ユーザーがアクセスできなくなった**
>
> 慎重に検討した結果、2024 年 7 月 25 AWS Cloud9日をもって、 への新しいお客様のアクセスを閉鎖することを決定しました。 AWS Cloud9 既存のお客様は、通常どおりサービスを引き続き使用できます。 AWS は引き続きセキュリティ、可用性、パフォーマンスの向上に投資しますが AWS Cloud9、新機能を導入する予定はありません。詳細については、「 から IDE Toolkits または AWS Cloud9AWS に移行する方法 AWS CloudShell」を参照してください。

AWS Cloud Map

AWS サービス	リソースタイプの値	関係	関連リソース
サービス検出	`AWS::ServiceDiscovery::Service`	NA	該当なし
	`AWS::ServiceDiscov`	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	ery::PublicDnsNamespace		
	AWS::ServiceDiscovery::HttpNamespace	該当なし	該当なし
AWS::ServiceDiscovery::Instance	該当なし	NA	

AWS CodeArtifact

AWS サービス	リソースタイプの値	関係	関連リソース
AWS CodeArtifact	AWS::CodeArtifact::Repository	NA	NA

AWS CodeBuild

AWS サービス	リソースタイプの値	関係	関連リソース
AWS CodeBuild	AWS::CodeBuild::Project *	is associated with	S3 バケット
			IAM ロール
	AWS::CodeBuild::ReportGroup	NA	NA

* と AWS Config の統合方法の詳細については AWS CodeBuild、「Use AWS Config with AWS CodeBuild Sample」を参照してください。

AWS CodeDeploy

AWS サービス	リソースタイプの値	関係	関連リソース
AWS CodeDeploy	`AWS::CodeDeploy::Application`	contains	DeploymentGroup
	`AWS::CodeDeploy::DeploymentConfig`	NA	NA
	`AWS::CodeDeploy::DeploymentGroup`	is contained in	アプリケーション

AWS CodePipeline

AWS サービス	リソースタイプの値	関係	関連リソース
AWS CodePipeline	`AWS::CodePipeline::Pipeline` *	is attached to	S3 バケット
		is associated with	IAM ロール
			コードプロジェクト
			Lambda function
			Cloudformation スタック
			ElasticBeanstalk アプリケーション

*AWS Config は、パイプライン内の CodePipeline パイプラインとサポートされているリソースタイプの設定変更を記録します。 は、まだサポートされていないパイプライン内のリソースタイプの設定変更を記録 AWS Config しません。`CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, や `ECS service` など、サポートされていないリソースタイプは、スタックの設定項目の補助的な設定セクションに表示されます。

AWS Config

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Config	`AWS::Config::ResourceCompliance` *	is associated with	すべてのリソース*
	`AWS::Config::ConformancePackCompliance`	NA	該当なし
	`AWS::Config::ConfigurationRecorder` *	該当なし	NA

*`AWS::Config::ResourceCompliance` と関連するリソースの関係は、`AWS::Config::ResourceCompliance` がその特定のリソースタイプのコンプライアンスをどのように報告するかによって異なります。

*`AWS::Config::ConfigurationRecorder` は のシステムリソースタイプ AWS Config であり、このリソースタイプの記録はデフォルトで有効になっています。

> **Note**
>
> `AWS::Config::ConformancePackCompliance` および `AWS::Config::ConfigurationRecorder` リソースタイプの記録は、追加料金なしでご利用いただけます。

AWS Database Migration Service

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Database Migration Service	`AWS::DMS::EventSubscription`	NA	該当なし
	`AWS::DMS::ReplicationSubnetGroup`	該当なし	該当なし
	`AWS::DMS::ReplicationInstance`	該当なし	該当なし
	`AWS::DMS::ReplicationTask`	該当なし	該当なし
	`AWS::DMS::Certificate`	該当なし	該当なし
	`AWS::DMS::Endpoint`	該当なし	NA

AWS DataSync

AWS サービス	リソースタイプの値	関係	関連リソース
AWS DataSync	`AWS::DataSync::LocationSMB`	NA	該当なし
	`AWS::DataSync::LocationFSxLustre`	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::DataSync::LocationFSxWindows	該当なし	該当なし
	AWS::DataSync::LocationS3	該当なし	該当なし
	AWS::DataSync::LocationEFS	該当なし	該当なし
	AWS::DataSync::LocationNFS	該当なし	該当なし
	AWS::DataSync::LocationHDFS	該当なし	該当なし
	AWS::DataSync::LocationObjectStorage	該当なし	該当なし
	AWS::DataSync::Task	該当なし	NA

AWS Device Farm

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Device Farm	`AWS::DeviceFarm::TestGridProject`	NA	該当なし
	`AWS::DeviceFarm::InstanceProfile`	該当なし	該当なし
	`AWS::DeviceFarm::Project`	該当なし	NA

AWS Elastic Beanstalk

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Application`	contains	Elastic Beanstalk アプリケーションバージョン
			Elastic Beanstalk 環境
		is associated with	IAM ロール
	`AWS::ElasticBeanstalk::ApplicationVersion`	is contained in	Elastic Beanstalk アプリケーション
		is associated with	Elastic Beanstalk 環境
			S3 バケット
	`AWS::ElasticBeanst`	is contained in	Elastic Beanstalk アプリケーション

AWS サービス	リソースタイプの値	関係	関連リソース
	`alk::Environment`	is associated with	Elastic Beanstalk アプリケーションバージョン
			IAM ロール
		contains	CloudFormation スタック

AWS Entity Resolution

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Entity Resolution	`AWS::EntityResolution::IdMappingWorkflow`	NA	該当なし
	`AWS::EntityResolution::SchemaMapping`	該当なし	NA

AWS Fault Injection Service

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Fault Injection Service	`AWS::FIS::ExperimentTemplate`	NA	NA

AWS Global Accelerator

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	NA	該当なし
	`AWS::GlobalAccelerator::EndpointGroup`	該当なし	該当なし
	`AWS::GlobalAccelerator::Accelerator`	該当なし	NA

AWS Glue

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Glue	`AWS::Glue::Job`	NA	該当なし
	`AWS::Glue::Classifier`	該当なし	該当なし
	`AWS::Glue::MLTransform`	該当なし	NA

AWS Ground Station

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Ground Station	`AWS::GroundStation::Config`	NA	該当なし
	`AWS::GroundStation::MissionProfile`	該当なし	該当なし
	`AWS::GroundStation::DataflowEndpointGroup`	該当なし	NA

AWS HealthLake

AWS サービス	リソースタイプの値	関係	関連リソース
AWS HealthLake	`AWS::HealthLake::FHIRDatastore`	NA	NA

AWS Identity and Access Management (IAM)

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Identity and Access Management	`AWS::IAM::User`	is attached to	IAM グループ
			IAM カスタマー管理ポリシー

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::IAM::Group	contains	IAM ユーザー
		is attached to	IAM カスタマー管理ポリシー
	AWS::IAM::Role	is attached to	IAM カスタマー管理ポリシー
	AWS::IAM::Policy	is attached to	IAM ユーザー
			IAM グループ
			IAM ロール
	AWS::IAM::SAMLProvider	NA	該当なし
	AWS::IAM::ServerCertificate	該当なし	該当なし
	AWS::IAM::InstanceProfile	該当なし	該当なし
	AWS::IAM::OIDCProvider	該当なし	該当なし
AWS Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	該当なし	NA

AWS Config には、記録する設定の詳細を含むインラインポリシーが含まれています。インラインポリシーの詳細については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシー」を参照してください。

AWS IoT

AWS サービス	リソースタイプの値	関係	関連リソース
AWS IoT	AWS::IoT::AccountAuditConfiguration	NA	該当なし
	AWS::IoT::Authorizer	該当なし	該当なし
	AWS::IoT::CACertificate	該当なし	該当なし
	AWS::IoT::CustomMetric	該当なし	該当なし
	AWS::IoT::Dimension	該当なし	該当なし
	AWS::IoT::DomainConfiguration	該当なし	該当なし
	AWS::IoT::JobTemplate	該当なし	該当なし
	AWS::IoT::MitigationAction	該当なし	該当なし
	AWS::IoT::Policy	該当なし	該当なし
	AWS::IoT::ProvisioningTemplate	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::IoT::RoleAlias	該当なし	該当なし
	AWS::IoT::ScheduledAudit	該当なし	該当なし
	AWS::IoT::SecurityProfile	該当なし	該当なし
	AWS::IoTSiteWise::Gateway	該当なし	該当なし
AWS IoT Wireless	AWS::IoTWireless::ServiceProfile	該当なし	該当なし
	AWS::IoTWireless::MulticastGroup	該当なし	該当なし
	AWS::IoTWireless::FuotaTask	該当なし	該当なし
AWS IoT Core	AWS::IoT::FleetMetric	該当なし	該当なし
AWS IoT Analytics	AWS::IoTAnalytics::Datastore	該当なし	該当なし
	AWS::IoTAnalytics::Dataset	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::IoTAnalytics::Pipeline	該当なし	該当なし
	AWS::IoTAnalytics::Channel	該当なし	該当なし
AWS IoT Events	AWS::IoTEvents::Input	該当なし	該当なし
	AWS::IoTEvents::DetectorModel	該当なし	該当なし
	AWS::IoTEvents::AlarmModel	該当なし	該当なし
AWS IoT TwinMaker	AWS::IoTTwinMaker::Workspace	該当なし	該当なし
	AWS::IoTTwinMaker::Entity	該当なし	該当なし
	AWS::IoTTwinMaker::Scene	該当なし	該当なし
	AWS::IoTTwinMaker::SyncJob	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::IoTTwinMaker::ComponentType	該当なし	該当なし
AWS IoT SiteWise	AWS::IoTSiteWise::Dashboard	該当なし	該当なし
	AWS::IoTSiteWise::Project	該当なし	該当なし
	AWS::IoTSiteWise::Portal	該当なし	該当なし
	AWS::IoTSiteWise::AssetModel	該当なし	該当なし
AWS IoT Greengrass Version 2	AWS::GreengrassV2::ComponentVersion	該当なし	NA

AWS Key Management Service

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Key Management Service	AWS::KMS::Key	NA	該当なし
	AWS::KMS::Alias	該当なし	NA

AWS Lambda

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Lambda	`AWS::Lambda::Function`	is associated with	IAM ロール
			EC2 セキュリティグループ
		is contained in	EC2 サブネット
	`AWS::Lambda::CodeSigningConfig`	NA	NA

AWS Mainframe Modernization

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Mainframe Modernization	`AWS::M2::Environment`	NA	NA

AWS Network Firewall

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	is attached to	EC2 サブネット
		is associated with	NetworkFirewall FirewallPolicy
	`AWS::NetworkFirewall::FirewallPolicy`	is associated with	NetworkFirewall RuleGroup

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::NetworkFirewall::RuleGroup	NA	該当なし
	AWS::NetworkFirewall::TLSInspectionConfiguration	該当なし	該当なし
	AWS::NetworkFirewall::VpcEndpointAssociation	該当なし	NA

AWS Network Manager

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Network Manager	AWS::NetworkManager::TransitGatewayRegistration	NA	該当なし
	AWS::NetworkManager::Site	該当なし	該当なし
	AWS::NetworkManager::Device	該当なし	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	AWS::NetworkManager::Link	該当なし	該当なし
	AWS::NetworkManager::GlobalNetwork	該当なし	該当なし
	AWS::NetworkManager::CustomerGatewayAssociation	該当なし	該当なし
	AWS::NetworkManager::LinkAssociation	該当なし	該当なし
	AWS::NetworkManager::ConnectPeer	該当なし	NA

AWS Panorama

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Panorama	AWS::Panorama::Package	NA	NA

AWS Private Certificate Authority

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`	NA	該当なし
	`AWS::ACMPCA::CertificateAuthorityActivation`	該当なし	NA
AWS Private CA Active Directory 用 コネクタ	`AWS::PCAConnectorAD::DirectoryRegistration`	NA	NA

AWS Resilience Hub

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Resilience Hub	`AWS::ResilienceHub::ResiliencyPolicy`	NA	該当なし
	`AWS::ResilienceHub::App`	該当なし	NA

AWS Resource Explorer

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Resource Explorer	`AWS::ResourceExplorer2::Index`	NA	NA

AWS RoboMaker

AWS サービス	リソースタイプの値	関係	関連リソース
AWS RoboMaker	`AWS::RoboMaker::RobotApplicationVersion`	NA	該当なし
	`AWS::RoboMaker::RobotApplication`	該当なし	該当なし
	`AWS::RoboMaker::SimulationApplication`	該当なし	NA

AWS Signer

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Signer	`AWS::Signer::SigningProfile`	NA	NA

AWS Secrets Manager

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Secrets Manager	`AWS::SecretsManager::Secret`	is associated with	Lambda 関数
		is associated with	KMS キー

AWS Security Hub

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Security Hub	`AWS::SecurityHub::Standard`	NA	NA

AWS Service Catalog

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Service Catalog	`AWS::ServiceCatalog::CloudFormationProduct`	is contained in	ポートフォリオ
		is associated with	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationProvisionedProduct`	is associated with	ポートフォリオ
			CloudFormationProduct
			CloudFormationStack

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::ServiceCatalog::Portfolio`	contains	CloudFormationProduct

> **Note**
>
> AWS Service Catalog で を使用すると AWS Config、設定項目には、親製品の ARN ではなく子プロビジョニング製品の ARN が表示されます。これは、 AWS Service Catalog プロビジョニング済み製品が CloudFormation を通じて親プロビジョニング済み製品内のリソースとして機能する場合に発生します。リソース ID は、 AWS Config インターフェイスを通じて追跡可能です。

AWS Shield

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Shield	`AWS::Shield::Protection`	is associated with	Amazon CloudFront ディストリビューション
	`AWS::ShieldRegional::Protection`	is associated with	EC2 EIP
		is associated with	ElasticLoadBalancing バランサー
		is associated with	ElasticLoadBalancingV2 LoadBalancer

AWS Step Functions

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Step Functions	`AWS::Step Functions::Activity`	NA	該当なし
	`AWS::Step Functions::StateMachine`	該当なし	NA

AWS Systems Manager

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Systems Manager	`AWS::SSM::ManagedInstanceInventory` *	is associated with	EC2 インスタンス
	`AWS::SSM::PatchCompliance`	is associated with	マネージドインスタンスのインベントリ
	`AWS::SSM::AssociationCompliance`	is associated with	マネージドインスタンスのインベントリ
	`AWS::SSM::FileData`	is associated with	マネージドインスタンスのインベントリ
	`AWS::SSM::Document`	NA	NA

* マネージドインスタンスのインベントリの詳細については、「Recording Software Configuration for Managed Instances」を参照してください。

AWS Transfer Family

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Transfer Family	`AWS::Transfer::Agreement`	NA	該当なし
	`AWS::Transfer::Connector`	該当なし	該当なし
	`AWS::Transfer::Workflow`	該当なし	該当なし
	`AWS::Transfer::Certificate`	該当なし	該当なし
	`AWS::Transfer::Profile`	該当なし	NA

AWS WAF

AWS サービス	リソースタイプの値	関係	関連リソース
AWS WAF	`AWS::WAF::RateBasedRule`	NA	該当なし
	`AWS::WAF::Rule`	該当なし	NA
	`AWS::WAF::WebACL`	is associated with	WAF ルール
			WAF レートベースのルール

AWS サービス	リソースタイプの値	関係	関連リソース
			WAF Rulegroup
	`AWS::WAF::RuleGroup`	is associated with	WAF ルール
	`AWS::WAFRegional::RateBasedRule`	NA	該当なし
	`AWS::WAFRegional::Rule`	該当なし	NA
	`AWS::WAFRegional::WebACL`	is associated with	ElasticLoadBalancingV2 LoadBalancer
			WAFRegional ルール
			WAFRegional レートベースのルール
			WAFRegional Rulegroup
	`AWS::WAFRegional::RuleGroup`	is associated with	WAFRegional ルール
AWS WAF V2	`AWS::WAFv2::WebACL`	is associated with	ElasticLoadBalancingV2 LoadBalancer
			ApiGateway Stage
			WAFv2 IPSet
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup

AWS サービス	リソースタイプの値	関係	関連リソース
			WAFv2 ManagedRuleSet
	`AWS::WAFv2::RuleGroup`	is associated with	WAFv2 IPSet
			WAFv2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	is associated with	WAFv2 RuleGroup
	`AWS::WAFv2::IPSet`	NA	該当なし
	`AWS::WAFv2::RegexPatternSet`	該当なし	NA

AWS X-Ray

AWS サービス	リソースタイプの値	関係	関連リソース
AWS X-Ray	`AWS::XRay::EncryptionConfig`	NA	NA

エラスティックロードバランシング

AWS サービス	リソースタイプの値	関係	関連リソース
エラスティックロードバランシング	Application Load Balancer	is associated with	EC2 セキュリティグループ

AWS サービス	リソースタイプの値	関係	関連リソース
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	is attached to	サブネット
		is contained in	仮想プライベートクラウド (VPC)
	Application Load Balancer Listener `AWS::ElasticLoadBalancingV2::Listener`	NA	NA
	Classic Load Balancer `AWS::ElasticLoadBalancing::LoadBalancer`	is associated with	EC2 セキュリティグループ
		is attached to	サブネット
		is contained in	仮想プライベートクラウド (VPC)
	Network Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	NA	NA

AWS Elemental MediaConnect

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Elemental MediaConnect	`AWS::MediaConnect:`	NA	該当なし

AWS サービス	リソースタイプの値	関係	関連リソース
	:FlowEntitlement		
	AWS::MediaConnect::FlowVpcInterface	該当なし	該当なし
	AWS::MediaConnect::FlowSource	該当なし	該当なし
	AWS::MediaConnect::Gateway	該当なし	NA

AWS Elemental MediaPackage

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Elemental MediaPackage	AWS::MediaPackage::PackagingGroup	NA	該当なし
	AWS::MediaPackage::PackagingConfiguration	該当なし	NA

AWS Elemental MediaTailor

AWS サービス	リソースタイプの値	関係	関連リソース
AWS Elemental MediaTailor	`AWS::MediaTailor::PlaybackConfiguration`	NA	NA

利用可能なリージョン別リソースカバレッジ

北米および南米リージョン

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::ACM::Certificate	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ACMPCA::CertificateAuthority	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ACMPCA::CertificateAuthorityActivation	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::APS::RuleGroupsNamespace	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::AccessAnalyzer::Analyzer	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::AmazonMQ::Broker	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Amplify::App	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Amplify::Branch	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ApiGateway::RestApi	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ApiGateway::Stage	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ApiGatewayV2::Api	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ApiGatewayV2::Stage	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AppConfig::Application	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::AppConfig::ConfigurationProfile	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppConfig::DeploymentStrategy	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::AppConfig::Environment	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppConfig::ExtensionAssociation	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::AppConfig::HostedConfigurationVersion	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppFlow::Flow	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppIntegrations::Application	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::AppIntegrations::EventIntegration	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::AppMesh::GatewayRoute	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppMesh::Mesh	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppMesh::Route	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppMesh::VirtualGateway	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppMesh::VirtualNode	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppMesh::VirtualRouter	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::AppMesh::VirtualService	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppRunner::Service	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::AppRunner::VpcConnector	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::AppStream::Application	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppStream::DirectoryConfig	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppStream::Fleet	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::AppStream::Stack	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::AppSync::ApiCache	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::AppSync::GraphQLApi	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Athena::DataCatalog	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Athena::PreparedStatement	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Athena::WorkGroup	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::AuditManager::Assessment	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::AutoScaling::AutoScalingGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AutoScaling::LaunchConfiguration	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::AutoScaling::ScalingPolicy	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AutoScaling::ScheduledAction	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Auto Scaling::WarmPool	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Backup::BackupPlan	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Backup::BackupSelection	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Backup::BackupVault	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Backup::RecoveryPoint	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Backup::ReportPlan	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Batch::ComputeEnvironment	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Batch::JobQueue	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Batch::SchedulingPolicy	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Bedrock::Guardrail	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Bedrock::KnowledgeBase	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Budgets::BudgetsAction	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Cassandra::Keyspace	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Cloud9::EnvironmentEC2	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::CloudFormation::Stack	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::CloudFront::Distribution	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::CloudFront::StreamingDistribution	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::CloudTrail::Trail	はい	はい	はい	はい	はい	はい	はい	はい
AWS::CloudWatch::Alarm	はい	はい	はい	はい	はい	はい	はい	はい
AWS::CloudWatch::MetricStream	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::CodeArtifact::Repository	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::CodeBuild::Project	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::CodeBuild::ReportGroup	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::CodeDeploy::Application	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::CodeDeploy::DeploymentConfig	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::CodeDeploy::DeploymentGroup	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::CodeGuruProfiler::ProfilingGroup	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::CodeGuruReviewer::RepositoryAssociation	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::CodePipeline::Pipeline	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Cognito::IdentityPool	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Cognito::UserPool	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Cognito::UserPoolClient	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Cognito::UserPoolGroup	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Config::ConfigurationRecorder	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Config::ConformancePackCompliance	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Config::ResourceCompliance	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Connect::Instance	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Connect::PhoneNumber	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Connect::QuickConnect	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Connect::Rule	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Connect::User	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::CustomerProfiles::Domain	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::CustomerProfiles::ObjectType	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::DMS::Certificate	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DMS::Endpoint	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DMS::EventSubscription	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DMS::ReplicationInstance	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DMS::ReplicationSubnetGroup	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DMS::ReplicationTask	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DataSync::LocationEFS	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::DataSync::LocationFSxLustre	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DataSync::LocationFSxWindows	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DataSync::LocationHDFS	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DataSync::LocationNFS	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DataSync::LocationObjectStorage	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DataSync::LocationS3	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::DataSync::LocationSMB	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::DataSync::Task	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Detective::Graph	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::DeviceFarm::InstanceProfile	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::DeviceFarm::Project	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::DeviceFarm::TestGridProject	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::DynamoDB::Table	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::Capacity Reservation	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::CarrierGateway	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::EC2::ClientVpnEndpoint	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::ClientVpnTargetNetworkAssociation	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::CustomerGateway	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::DHCPOptions	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::EC2Fleet	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::EIP	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::EIPAssociation	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::EgressOnlyInternetGateway	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::EC2::FlowLog	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::Host	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::IPAM	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::IPAMPool	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::IPAMResourceDiscovery	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::IPAMResourceDiscoveryAssociation	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::IPAMScope	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::Instance	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::EC2::Instance ConnectEndpoint	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::InternetGateway	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::LaunchTemplate	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::NatGateway	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::NetworkAcl	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::NetworkInsightsAccessScope	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::NetworkInsightsAccessScopeAnalysis	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::NetworkInsightsAnalysis	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::EC2::NetworkInsightsPath	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::NetworkInterface	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::PrefixList	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::RegisteredHAInstance	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::RouteTable	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::SecurityGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::SnapshotBlockPublicAccess	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::SpotFleet	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::Subnet	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::EC2::SubnetRouteTableAssociation	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::TrafficMirrorFilter	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::TrafficMirrorSession	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::TrafficMirrorTarget	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::TransitGateway	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::TransitGatewayAttachment	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::TransitGatewayConnect	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::EC2::TransitGatewayMulticastDomain	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::TransitGatewayRouteTable	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EC2::VPC	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCBlockPublicAccessExclusion	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::VPCBlockPublicAccessOptions	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::VPCEndpoint	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCEndpointConnectionNotification	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCEndpointService	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCPeeringConnection	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::EC2::VPNConnection	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPNConnectionRoute	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::VPNGateway	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::Volume	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECR::PublicRepository	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::ECR::PullThroughCacheRule	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ECR::RegistryPolicy	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ECR::Repository	はい	はい	はい	はい	はい	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::ECS::CapacityProvider	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ECS::Cluster	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::Service	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::TaskDefinition	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::TaskSet	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EFS::AccessPoint	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EFS::FileSystem	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EKS::Addon	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::EKS::Cluster	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EKS::FargateProfile	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EKS::IdentityProviderConfig	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EMR::SecurityConfiguration	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ElasticBeanstalk::Application	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ElasticBeanstalk::ApplicationVersion	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ElasticBeanstalk::Environment	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ElasticLoadBalancing::LoadBalancer	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::ElasticLoadBalancingV2::Listener	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ElasticLoadBalancingV2::LoadBalancer	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Elasticsearch::Domain	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EventSchemas::Discoverer	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EventSchemas::Registry	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EventSchemas::RegistryPolicy	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::EventSchemas::Schema	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Events::ApiDestination	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Events::Archive	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Events::Connection	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Events::Endpoint	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Events::EventBus	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Events::Rule	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Evidently::Launch	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::Evidently::Project	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Evidently::Segment	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::FIS::ExperimentTemplate	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Forecast::Dataset	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::Forecast::DatasetGroup	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::FraudDetector::EntityType	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::FraudDetector::Label	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::FraudDetector::Outcome	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::FraudDetector::Variable	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::GlobalAccelerator::Accelerator	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::GlobalAccelerator::EndpointGroup	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::GlobalAccelerator::Listener	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Glue::Classifier	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Glue::Job	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Glue::MLTransform	はい	はい	はい	はい	はい	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Grafana::Workspace	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::GreengrassV2::ComponentVersion	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::GroundStation::Config	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	はい
AWS::GroundStation::DataflowEndpointGroup	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	はい
AWS::GroundStation::MissionProfile	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	はい
AWS::GuardDuty::Detector	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::GuardDuty::Filter	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::GuardDuty::IPSet	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::GuardDuty::ThreatIntelSet	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::HealthLake::FHIRDatastore	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::IAM::Group	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::IAM::InstanceProfile	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IAM::OIDCProvider	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IAM::Policy	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::IAM::Role	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::IAM::SAMLProvider	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IAM::ServerCertificate	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IAM::User	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::IVS::Channel	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IVS::PlaybackKeyPair	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IVS::RecordingConfiguration	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::ImageBuilder::ContainerRecipe	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ImageBuilder::DistributionConfiguration	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ImageBuilder::ImagePipeline	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ImageBuilder::ImageRecipe	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ImageBuilder::InfrastructureConfiguration	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::InspectorV2::Activation	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::InspectorV2::Filter	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::IoT::AccountAuditConfiguration	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoT::Authorizer	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::IoT::CACertificate	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::IoT::CustomMetric	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoT::Dimension	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoT::FleetMetric	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::IoT::JobTemplate	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::IoT::MitigationAction	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoT::Policy	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::IoT::ProvisioningTemplate	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::IoT::RoleAlias	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::IoT::ScheduledAudit	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoT::SecurityProfile	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoTAnalytics::Channel	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::IoTAnalytics::Dataset	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::IoTAnalytics::Datastore	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::IoTAnalytics::Pipeline	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::IoTEvents::AlarmModel	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoTEvents::DetectorModel	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoTEvents::Input	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoTSiteWise::AssetModel	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::IoTSiteWise::Dashboard	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoTSiteWise::Gateway	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoTSiteWise::Portal	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoTSiteWise::Project	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::IoTTwinMaker::ComponentType	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTTwinMaker::Entity	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTTwinMaker::Scene	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::IoTTwinMaker::SyncJob	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTTwinMaker::Workspace	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS:: IoTWireless:: FuotaTask	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	はい
AWS::IoTWireless::MulticastGroup	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	はい
AWS::IoTWireless::ServiceProfile	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	はい
AWS::KMS::Alias	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::KMS::Key	はい	はい	はい	はい	はい	はい	はい	はい
AWS::KafkaConnect::Connector	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Kendra::Index	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::Kinesis::Stream	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Kinesis::StreamConsumer	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::KinesisAnalyticsV2::Application	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::KinesisFirehose::DeliveryStream	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::KinesisVideo::SignalingChannel	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::KinesisVideo::Stream	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Lambda::CodeSigningConfig	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Lambda::Function	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Lex::Bot	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Lex::BotAlias	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Lightsail::Bucket	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::Lightsail::Certificate	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::Lightsail::Disk	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::Lightsail::StaticIp	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Logs::Destination	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::LookoutMetrics::Alert	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::LookoutVision::Project	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::M2::Environment	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MSK::BatchScramSecret	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MSK::Cluster	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MSK::ClusterPolicy	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::MSK::Configuration	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::MSK::VpcConnection	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Macie::Session	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MediaConnect::FlowEntitlement	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MediaConnect::FlowSource	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MediaConnect::FlowVpcInterface	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MediaConnect::Gateway	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::MediaPackage::PackagingConfiguration	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MediaPackage::PackagingGroup	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MediaTailor::PlaybackConfiguration	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::MemoryDB::SubnetGroup	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::NetworkFirewall::Firewall	はい	はい	はい	はい	はい	はい	はい	はい
AWS::NetworkFirewall::FirewallPolicy	はい	はい	はい	はい	はい	はい	はい	はい
AWS::NetworkFirewall::RuleGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::NetworkFirewall::TLSInspectionConfiguration	はい	はい	はい	はい	はい	はい	はい	はい
AWS::NetworkFirewall::VpcEndpointAssociation	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::NetworkManager::ConnectPeer	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::NetworkManager::CustomerGatewayAssociation	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::NetworkManager::Device	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::NetworkManager::GlobalNetwork	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::NetworkManager::Link	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::NetworkManager::LinkAssociation	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::NetworkManager::Site	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::NetworkManager::TransitGatewayRegistration	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::OpenSearch::Domain	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::OpenSearchServerless::Collection	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::OpenSearchServerless::VpcEndpoint	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Panorama::Package	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Personalize::Dataset	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::Personalize::DatasetGroup	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Personalize::Schema	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::Personalize::Solution	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::Pinpoint::App	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Pinpoint::ApplicationSettings	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Pinpoint::Campaign	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Pinpoint::EmailChannel	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Pinpoint::EmailTemplate	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Pinpoint::EventStream	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::Pinpoint::InAppTemplate	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::Pinpoint::Segment	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
AWS::QLDB::Ledger	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::QuickSight::DataSource	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::QuickSight::Template	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::QuickSight::Theme	いいえ	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::RDS::DBCluster	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::RDS::DBClusterSnapshot	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBInstance	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBSecurityGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBSnapshot	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBSubnetGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::EventSubscription	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::GlobalCluster	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::RDS::OptionGroup	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::RUM::AppMonitor	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Redshift::Cluster	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterParameterGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterSecurityGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterSnapshot	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterSubnetGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::EndpointAccess	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Redshift::EndpointAuthorization	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Redshift::EventSubscription	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ScheduledAction	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::ResilienceHub::App	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ResilienceHub::ResiliencyPolicy	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ResourceExplorer2::Index	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::RoboMaker::RobotApplication	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::RoboMaker::RobotApplicationVersion	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::RoboMaker::SimulationApplication	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::Route53::HealthCheck	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Route53::HostedZone	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Route53Profiles::Profile	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Route53RecoveryControl::Cluster	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Route53RecoveryControl::ControlPanel	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Route53RecoveryControl::RoutingControl	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Route53RecoveryControl::SafetyRule	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Route53RecoveryReadiness::Cell	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Route53RecoveryReadiness::ReadinessCheck	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Route53RecoveryReadiness::RecoveryGroup	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Route53RecoveryReadiness::ResourceSet	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Route53Resolver::FirewallDomainList	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Route53Resolver::FirewallRuleGroup	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Route53Resolver::FirewallRuleGroupAssociation	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Route53Resolver::ResolverEndpoint	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Route53Resolver::ResolverQueryLoggingConfig	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Route53Resolver::ResolverRule	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Route53Resolver::ResolverRuleAssociation	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::S3::AccessPoint	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::S3::AccountPublicAccessBlock	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::S3::Bucket	はい	はい	はい	はい	はい	はい	はい	はい
AWS::S3::MultiRegionAccessPoint	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::S3::StorageLens	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::S3::StorageLensGroup	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::S3Express::BucketPolicy	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::S3Express::DirectoryBucket	いいえ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::SES::ConfigurationSet	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SES::ContactList	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SES::ReceiptFilter	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::SES::ReceiptRuleSet	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::SES::Template	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SNS::Topic	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SQS::Queue	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SSM::AssociationCompliance	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SSM::Document	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::SSM::FileData	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SSM::ManagedInstanceInventory	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SSM::PatchCompliance	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::SageMaker::AppImageConfig	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SageMaker::CodeRepository	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SageMaker::Domain	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SageMaker::EndpointConfig	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SageMaker::FeatureGroup	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SageMaker::Image	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SageMaker::InferenceExperiment	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::SageMaker::Model	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SageMaker::NotebookInstance	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SageMaker::NotebookInstanceLifecycleConfig	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::SageMaker::Workteam	いいえ	はい	はい	はい	いいえ	はい	いいえ	いいえ
AWS::SecretsManager::Secret	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SecurityHub::Standard	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ServiceCatalog::CloudFormationProduct	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ServiceCatalog::CloudFormationProvisionedProduct	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::ServiceCatalog::Portfolio	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ServiceDiscovery::HttpNamespace	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ServiceDiscovery::Instance	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::ServiceDiscovery::PublicDnsNamespace	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::ServiceDiscovery::Service	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Shield::Protection	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::ShieldRegional::Protection	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Signer::SigningProfile	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Step Functions::Activity	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::StepFunctions::StateMachine	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Transfer::Agreement	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::Transfer::Certificate	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Transfer::Connector	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Transfer::Profile	はい	はい	はい	はい	はい	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::Transfer::Workflow	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::WAF::RateBasedRule	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::WAF::Rule	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::WAF::RuleGroup	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::WAF::WebACL	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::WAFRegional::RateBasedRule	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::WAFRegional::Rule	はい	はい	はい	はい	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::WAFRegional::RuleGroup	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::WAFRegional::WebACL	はい	はい	はい	はい	いいえ	はい	いいえ	はい
AWS::WAFv2::IPSet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFv2::ManagedRuleSet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFv2::RegexPatternSet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFv2::RuleGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFv2::WebACL	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WorkSpaces::ConnectionAlias	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	はい
AWS::WorkSpaces::Workspace	いいえ	はい	はい	いいえ	いいえ	はい	いいえ	はい

リソースタイプ	米国西部(北カリフォルニア)	米国東部(バージニア北部)	米国西部(オレゴン)	米国東部(オハイオ)	カナダ西部(カルガリー)	カナダ(中部)	メキシコ(中部)	南米(サンパウロ)
AWS::XRay::EncryptionConfig	はい	はい	はい	はい	いいえ	はい	いいえ	はい

欧州リージョン

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::ACM::Certificate	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ACMPCA::CertificateAuthority	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ACMPCA::CertificateAuthorityActivation	はい	はい	はい	はい	はい	はい	はい	はい
AWS::APS::RuleGroupsNamespace	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::AccessAnalyzer::Analyzer	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::AmazonMQ::Broker	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Amplify::App	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Amplify::Branch	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ApiGateway::RestApi	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ApiGateway::Stage	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ApiGatewayV2::Api	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ApiGatewayV2::Stage	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AppConfig::Application	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::AppConfig::ConfigurationProfile	はい	はい	はい	はい	はい	はい	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::AppConfig::DeploymentStrategy	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AppConfig::Environment	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::AppConfig::ExtensionAssociation	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AppConfig::HostedConfigurationVersion	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::AppFlow::Flow	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::AppIntegrations::Application	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::AppIntegrations::EventIntegration	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::AppMesh::GatewayRoute	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::AppMesh::Mesh	はい	はい	はい	はい	はい	はい	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::AppMesh::Route	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::AppMesh::VirtualGateway	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::AppMesh::VirtualNode	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::AppMesh::VirtualRouter	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::AppMesh::VirtualService	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::AppRunner::Service	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::AppRunner::VpcConnector	はい	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ
AWS::AppStream::Application	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::AppStream::DirectoryConfig	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::AppStream::Fleet	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::AppStream::Stack	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::AppSync::ApiCache	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AppSync::GraphQLApi	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Athena::DataCatalog	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Athena::PreparedStatement	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::Athena::WorkGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AuditManager::Assessment	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::AutoScaling::AutoScalingGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AutoScaling::LaunchConfiguration	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AutoScaling::ScalingPolicy	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AutoScaling::ScheduledAction	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Auto Scaling::WarmPool	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Backup::BackupPlan	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Back up::BackupSelection	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Backup::BackupVault	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Back up::RecoveryPoint	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Backup::ReportPlan	はい	はい	はい	はい	はい	はい	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::Batch::ComputeEnvironment	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Batch::JobQueue	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Batch::SchedulingPolicy	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Bedrock::Guardrail	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Bedrock::KnowledgeBase	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Cassandra::Keyspace	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::Cloud9::EnvironmentEC2	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::CloudFormation::Stack	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::CloudTrail::Trail	はい	はい	はい	はい	はい	はい	はい	はい
AWS::CloudWatch::Alarm	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::CloudWatch::MetricStream	はい	はい	はい	はい	はい	はい	はい	はい
AWS::CodeArtifact::Repository	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::CodeBuild::Project	はい	はい	はい	はい	はい	はい	はい	はい
AWS::CodeBuild::ReportGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::CodeDeploy::Application	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::CodeDeploy::DeploymentConfig	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::CodeDeploy::DeploymentGroup	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::CodeGuruProfiler::ProfilingGroup	はい	はい	はい	いいえ	はい	いいえ	いいえ	いいえ
AWS::CodeGuruReviewer::RepositoryAssociation	はい	はい	はい	いいえ	はい	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::CodePipeline::Pipeline	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Cognito::IdentityPool	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Cognito::UserPool	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Cognito::UserPoolClient	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Cognito::UserPoolGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Config::ConfigurationRecorder	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Config::ConformancePackCompliance	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Config::ResourceCompliance	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Connect::Instance	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Connect::PhoneNumber	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::Connect::QuickConnect	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Connect::Rule	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Connect::User	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::CustomerProfiles::Domain	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::CustomerProfiles::ObjectType	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::DMS::Certificate	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::DMS::Endpoint	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::DMS::EventSubscription	はい	はい	はい	はい	はい	はい	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::DMS::ReplicationInstance	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::DMS::ReplicationSubnetGroup	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::DMS::ReplicationTask	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::DataSync::LocationEFS	はい	はい	はい	はい	はい	はい	はい	はい
AWS::DataSync::LocationFSxLustre	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::DataSync::LocationFSxWindows	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::DataSync::LocationHDFS	はい	はい	はい	はい	はい	はい	はい	はい
AWS::DataSync::LocationNFS	はい	はい	はい	はい	はい	はい	はい	はい
AWS::DataSync::LocationObjectStorage	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::DataSync::LocationS3	はい	はい	はい	はい	はい	はい	はい	はい
AWS::DataSync::LocationSMB	はい	はい	はい	はい	はい	はい	はい	はい
AWS::DataSync::Task	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Detective::Graph	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::DynamoDB::Table	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::CapacityReservation	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::CarrierGateway	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::EC2::ClientVpnEndpoint	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::ClientVpnTargetNetworkAssociation	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::CustomerGateway	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::EC2::DHCPOptions	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::EC2Fleet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::EIP	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::EIPAssociation	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::EgressOnlyInternetGateway	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::FlowLog	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::Host	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::IPAM	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::IPAMPool	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::IPAMResourceDiscovery	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::EC2::IPAMResourceDiscoveryAssociation	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::IPAMScope	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::Instance	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::InstanceConnectEndpoint	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::InternetGateway	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::LaunchTemplate	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::EC2::NatGateway	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::NetworkAcl	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::NetworkInsightsAccessScope	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::EC2::NetworkInsightsAccessScopeAnalysis	はい	はい	はい	はい	はい	はい	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::EC2::NetworkInsightsAnalysis	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::EC2::NetworkInsightsPath	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::EC2::NetworkInterface	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::PrefixList	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::RegisteredHAInstance	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::EC2::RouteTable	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::SecurityGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::SnapshotBlockPublicAccess	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::SpotFleet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::Subnet	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::EC2::SubnetRouteTableAssociation	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::TrafficMirrorFilter	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::TrafficMirrorSession	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::TrafficMirrorTarget	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::TransitGateway	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::TransitGatewayAttachment	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::TransitGatewayConnect	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::TransitGatewayMulticastDomain	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::TransitGatewayRouteTable	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::EC2::VPC	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::EC2::VPCBlockPublicAccessExclusion	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCBlockPublicAccessOptions	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCEndpoint	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCEndpointConnectionNotification	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCEndpointService	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCPeeringConnection	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPNConnection	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPNConnectionRoute	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPNGateway	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::Volume	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECR::PullThroughCacheRule	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::ECR::RegistryPolicy	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECR::Repository	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::CapacityProvider	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::Cluster	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::Service	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::TaskDefinition	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::TaskSet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EFS::AccessPoint	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EFS::FileSystem	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EKS::Addon	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EKS::Cluster	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::EKS::FargateProfile	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EKS::IdentityProviderConfig	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EMR::SecurityConfiguration	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ElasticBeanstalk::Application	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ElasticBeanstalk::ApplicationVersion	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ElasticBeanstalk::Environment	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ElasticLoadBalancing::LoadBalancer	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ElasticLoadBalancingV2::Listener	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ElasticLoadBalancingV2::LoadBalancer	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Elasticsearch::Domain	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::EventSchemas::Discoverer	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EventSchemas::Registry	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EventSchemas::RegistryPolicy	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EventSchemas::Schema	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Events::ApiDestination	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Events::Archive	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Events::Connection	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Events::Endpoint	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::Events::EventBus	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Events::Rule	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::Evidently::Launch	はい	はい	いいえ	いいえ	はい	いいえ	いいえ	いいえ
AWS::Evidently::Project	はい	はい	いいえ	いいえ	はい	いいえ	いいえ	いいえ
AWS::Evidently::Segment	はい	はい	いいえ	いいえ	はい	いいえ	いいえ	いいえ
AWS::FIS::ExperimentTemplate	はい	はい	はい	はい	はい	はい	はい	いいえ
AWS::Forecast::Dataset	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Forecast::DatasetGroup	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::FraudDetector::EntityType	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::FraudDetector::Label	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::FraudDetector::Outcome	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::FraudDetector::Variable	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Glue::Classifier	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Glue::Job	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Glue::MLTransform	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Grafana::Workspace	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::GreengrassV2::ComponentVersion	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::GroundStation::Config	はい	はい	いいえ	いいえ	はい	いいえ	いいえ	いいえ
AWS::GroundStation::DataflowEndpointGroup	はい	はい	いいえ	いいえ	はい	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::GroundStation::MissionProfile	はい	はい	いいえ	いいえ	はい	いいえ	いいえ	いいえ
AWS::GuardDuty::Detector	はい	はい	はい	はい	はい	はい	はい	はい
AWS::GuardDuty::Filter	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::GuardDuty::IPSet	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::GuardDuty::ThreatIntelSet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::IAM::Group	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::IAM::Policy	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::IAM::Role	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::IAM::User	はい	はい	はい	はい	はい	はい	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::IVS::Channel	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IVS::PlaybackKeyPair	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IVS::RecordingConfiguration	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::ImageBuilder::ContainerRecipe	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ImageBuilder::DistributionConfiguration	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ImageBuilder::ImagePipeline	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ImageBuilder::ImageRecipe	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ImageBuilder::InfrastructureConfiguration	はい	はい	はい	はい	はい	はい	はい	はい
AWS::InspectorV2::Activation	はい	はい	はい	はい	はい	はい	いいえ	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::InspectorV2::Filter	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::IoT::AccountAuditConfiguration	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::Authorizer	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::CACertificate	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::CustomMetric	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::Dimension	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::FleetMetric	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::JobTemplate	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::IoT::MitigationAction	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::Policy	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::ProvisioningTemplate	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::RoleAlias	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::ScheduledAudit	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoT::SecurityProfile	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::IoTAnalytics::Channel	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTAnalytics::Dataset	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::IoTAnalytics::Datastore	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTAnalytics::Pipeline	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTEvents::AlarmModel	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTEvents::DetectorModel	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTEvents::Input	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTSiteWise::AssetModel	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTSiteWise::Dashboard	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTSiteWise::Gateway	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::IoTSiteWise::Portal	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTSiteWise::Project	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTTwinMaker::ComponentType	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTTwinMaker::Entity	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTTwinMaker::Scene	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTTwinMaker::SyncJob	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTTwinMaker::Workspace	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS:: IoTWireless:: FuotaTask	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::IoTWireless::MulticastGroup	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IoTWireless::ServiceProfile	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::KMS::Alias	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::KMS::Key	はい	はい	はい	はい	はい	はい	はい	はい
AWS::KafkaConnect::Connector	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::Kendra::Index	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Kinesis::Stream	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Kinesis::StreamConsumer	はい	はい	はい	はい	はい	はい	はい	はい
AWS::KinesisAnalyticsV2::Application	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::KinesisFirehose::DeliveryStream	はい	はい	はい	はい	はい	はい	はい	はい
AWS::KinesisVideo::SignalingChannel	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::KinesisVideo::Stream	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::Lambda::CodeSigningConfig	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Lambda::Function	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Lex::Bot	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Lex::BotAlias	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Lightsail::Bucket	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::Lightsail::Certificate	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::Lightsail::Disk	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::Lightsail::StaticIp	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::Logs::Destination	はい	はい	はい	はい	はい	はい	はい	はい
AWS::LookoutMetrics::Alert	はい	はい	いいえ	いいえ	はい	いいえ	いいえ	いいえ
AWS::LookoutVision::Project	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::M2::Environment	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::MSK::BatchScramSecret	はい	はい	はい	はい	はい	はい	はい	はい
AWS::MSK::Cluster	はい	はい	はい	はい	はい	はい	はい	はい
AWS::MSK::ClusterPolicy	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::MSK::Configuration	はい	はい	はい	はい	はい	はい	はい	はい
AWS::MSK::VpcConnection	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Macie::Session	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::MediaConnect::FlowEntitlement	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::MediaConnect::FlowSource	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::MediaConnect::FlowVpcInterface	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::MediaConnect::Gateway	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::MediaPackage::PackagingConfiguration	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::MediaPackage::PackagingGroup	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::MediaTailor::PlaybackConfiguration	はい	はい	いいえ	はい	はい	いいえ	いいえ	いいえ
AWS::MemoryDB::SubnetGroup	はい	はい	はい	いいえ	はい	いいえ	いいえ	いいえ
AWS::NetworkFirewall::Firewall	はい	はい	はい	はい	はい	はい	はい	はい
AWS::NetworkFirewall::FirewallPolicy	はい	はい	はい	はい	はい	はい	はい	はい
AWS::NetworkFirewall::RuleGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::NetworkFirewall::TLSInspectionConfiguration	はい	はい	はい	はい	はい	はい	はい	はい
AWS::NetworkFirewall::VpcEndpointAssociation	はい	はい	はい	はい	はい	はい	はい	はい
AWS::OpenSearch::Domain	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::OpenSearchServerless::Collection	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::OpenSearchServerless::VpcEndpoint	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
AWS::Panorama::Package	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Personalize::Dataset	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Personalize::DatasetGroup	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Personalize::Schema	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Personalize::Solution	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Pinpoint::App	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Pinpoint::ApplicationSettings	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::Pinpoint::Campaign	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Pinpoint::EmailChannel	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Pinpoint::EmailTemplate	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Pinpoint::EventStream	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Pinpoint::InAppTemplate	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Pinpoint::Segment	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::QLDB::Ledger	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::QuickSight::DataSource	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::QuickSight::Template	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::QuickSight::Theme	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::RDS::DBCluster	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBClusterSnapshot	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBInstance	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBSecurityGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBSnapshot	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBSubnetGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::EventSubscription	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::GlobalCluster	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::RDS::OptionGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RUM::AppMonitor	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::Cluster	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterParameterGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterSecurityGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterSnapshot	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterSubnetGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::EndpointAccess	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::Redshift::EndpointAuthorization	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::Redshift::EventSubscription	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::Redshift::ScheduledAction	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ResilienceHub::App	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ResilienceHub::ResiliencyPolicy	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ResourceExplorer2::Index	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RoboMaker::RobotApplication	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::RoboMaker::RobotApplicationVersion	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::RoboMaker::SimulationApplication	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::Route53Profiles::Profile	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Route53Resolver::FirewallDomainList	はい	はい	はい	はい	はい	はい	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::Route53Resolver::FirewallRuleGroup	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Route53Resolver::FirewallRuleGroupAssociation	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Route53Resolver::ResolverEndpoint	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Route53Resolver::ResolverQueryLoggingConfig	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Route53Resolver::ResolverRule	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Route53Resolver::ResolverRuleAssociation	はい	はい	はい	はい	はい	はい	はい	はい
AWS::S3::AccessPoint	はい	はい	はい	はい	はい	はい	はい	はい
AWS::S3::AccountPublicAccessBlock	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::S3::Bucket	はい	はい	はい	はい	はい	はい	はい	はい
AWS::S3::StorageLens	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::S3::StorageLensGroup	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ
AWS::S3Express::BucketPolicy	はい	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ
AWS::S3Express::DirectoryBucket	はい	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ
AWS::SES::ConfigurationSet	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SES::ContactList	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SES::ReceiptFilter	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::SES::ReceiptRuleSet	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::SES::Template	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SNS::Topic	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SQS::Queue	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SSM::AssociationCompliance	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SSM::Document	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SSM::FileData	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SSM::ManagedInstanceInventory	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SSM::PatchCompliance	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SageMaker::AppImageConfig	はい	はい	はい	はい	はい	はい	はい	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::SageMaker::CodeRepository	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SageMaker::Domain	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SageMaker::EndpointConfig	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SageMaker::FeatureGroup	はい	はい	はい	はい	はい	はい	はい	いいえ
AWS::SageMaker::Image	はい	はい	はい	はい	はい	はい	はい	いいえ
AWS::SageMaker::InferenceExperiment	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SageMaker::Model	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SageMaker::NotebookInstance	はい	はい	はい	はい	はい	はい	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::SageMaker::NotebookInstanceLifecycleConfig	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::SageMaker::Workteam	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::SecretsManager::Secret	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SecurityHub::Standard	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ServiceCatalog::CloudFormationProduct	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ServiceCatalog::CloudFormationProvisionedProduct	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ServiceCatalog::Portfolio	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ServiceDiscovery::HttpNamespace	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ServiceDiscovery::Instance	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ServiceDiscovery::PublicDnsNamespace	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::ServiceDiscovery::Service	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::ShieldRegional::Protection	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Signer::SigningProfile	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::StepFunctions::Activity	はい	はい	はい	はい	はい	はい	はい	はい
AWS::StepFunctions::StateMachine	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Transfer::Agreement	はい	はい	はい	はい	はい	はい	いいえ	いいえ
AWS::Transfer::Certificate	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Transfer::Connector	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Transfer::Profile	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Transfer::Workflow	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::WAFRegional::RateBasedRule	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFRegional::Rule	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFRegional::RuleGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFRegional::WebACL	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFv2::IPSet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFv2::ManagedRuleSet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFv2::RegexPatternSet	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFv2::RuleGroup	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WAFv2::WebACL	はい	はい	はい	はい	はい	はい	はい	はい
AWS::WorkSpaces::ConnectionAlias	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

リソースタイプ	欧州(アイルランド)	欧州(フランクフルト)	欧州(ロンドン)	欧州(パリ)	欧州(ストックホルム)	欧州(ミラノ)	欧州(スペイン)	欧州(チューリッヒ)
AWS::WorkSpaces::Workspace	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::XRay::EncryptionConfig	はい	はい	はい	はい	はい	はい	はい	はい

アジアパシフィックリージョン

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::ACM::Certificate	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ACMPCA::CertificateAuthority	はい	はい	はい	い	はい	はい	はい	はい	はい	はい	い	い	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
				いえ							いえ	いえ	
AWS::ACMPCA::CertificateAuthorityActivation	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::APS::RuleGroupsNamespace	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::AccessAnalyzer::Analyzer	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AmazonMQ::Broker	はい	いいえ	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Amplify::App	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Amplify::Branch	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ApiGateway::RestApi	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::ApiGateway::Stage	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::ApiGatewayV2::Api	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::ApiGatewayV2::Stage	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::AppConfig::Application	はい	いいえ	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppConfig::ConfigurationProfile	はい	いいえ	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::AppConfig::DeploymentStrategy	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppConfig::Environment	はい	いいえ	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppConfig::ExtensionAssociation	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppConfig::HostedConfigurationVersion	はい	いいえ	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::AppFlow::Flow	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::AppIntegrations::Application	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::AppIntegrations::EventIntegration	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::AppMesh::GatewayRoute	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::AppMesh::Mesh	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppMesh::Route	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppMesh::VirtualGateway	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppMesh::VirtualNode	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::AppMesh::VirtualRouter	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppMesh::VirtualService	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppRunner::Service	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::AppRunner::VpcConnector	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::AppStream::Application	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::AppStream::DirectoryConfig	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::AppStream::Fleet	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::AppStream::Stack	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::AppSync::ApiCache	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AppSync::GraphQLApi	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Athena::DataCatalog	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Athena::PreparedStatement	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Athena::WorkGroup	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::AuditManager::Assessment	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::AutoScaling::AutoScalingGroup	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AutoScaling::LaunchConfiguration	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::AutoScaling::ScalingPolicy	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Auto Scaling::ScheduledAction	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Auto Scaling::WarmPool	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Backup::BackupPlan	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Backup::BackupSelection	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Backup::BackupVault	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Backup::RecoveryPoint	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Backup::ReportPlan	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Batch::ComputeEnvironment	はい	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Batch::JobQueue	はい	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Batch::SchedulingPolicy	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Bedrock::Guardrail	いいえ	はい	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	はい
AWS::Bedrock::KnowledgeBase	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	はい	いいえ	はい
AWS::Cassandra::Keyspace	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Cloud9::EnvironmentEC2	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::CloudFormation::Stack	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::CloudTrail::Trail	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::CloudWatch::Alarm	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::CloudWatch::MetricStream	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::CodeArtifact::Repository	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::CodeBuild::Project	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::CodeBuild::ReportGroup	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::CodeDeploy::Application	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::CodeDeploy::DeploymentConfig	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::CodeDeploy::DeploymentGroup	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::CodeGuruProfiler::ProfilingGroup	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::CodeGuruReviewer::RepositoryAssociation	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::CodePipeline::Pipeline	はい	はい	いいえ	いいえ	はい	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Cognito::IdentityPool	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Cognito::UserPool	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Cognito::UserPoolClient	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Cognito::UserPoolGroup	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Config::ConfigurationRecorder	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Config::ConformancePackCompliance	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Config::ResourceCompliance	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Connect::Instance	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Connect::PhoneNumber	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Connect::QuickConnect	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Connect::Rule	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Connect::User	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::CustomerProfiles::Domain	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::CustomerProfiles::ObjectType	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::DMS::Certificate	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DMS::Endpoint	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::DMS::EventSubscription	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DMS::ReplicationInstance	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DMS::ReplicationSubnetGroup	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DMS::ReplicationTask	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::DataSync::LocationEFS	はい	いいえ	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DataSync::LocationFSxLustre	はい	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DataSync::LocationFSxWindows	はい	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DataSync::LocationHDFS	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::DataSync::LocationNFS	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DataSync::LocationObjectStorage	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DataSync::LocationS3	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::DataSync::LocationSMB	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::DataSync::Task	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Detective::Graph	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::DynamoDB::Table	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::CapacityReservation	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::CarrierGateway	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::ClientVpnEndpoint	はい	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::ClientVpnTargetNetworkAssociation	はい	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::CustomerGateway	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::DHCPOptions	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::EC2Fleet	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::EIP	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::EIPAssociation	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::EC2::EgressOnlyInternetGateway	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::FlowLog	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::Host	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::IPAM	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::IPAMPool	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::IPAMResourceDiscovery	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::IPAMResourceDiscoveryAssociation	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::IPAMScope	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::Instance	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::InstanceConnectEndpoint	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::InternetGateway	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::LaunchTemplate	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::NatGateway	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::NetworkAcl	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::NetworkInsightsAccessScope	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::NetworkInsightsAccessScopeAnalysis	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::NetworkInsightsAnalysis	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::NetworkInsightsPath	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::NetworkInterface	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::PrefixList	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::RegisteredHAInstance	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::RouteTable	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::SecurityGroup	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::SnapshotBlockPublicAccess	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::SpotFleet	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::Subnet	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::SubnetRouteTableAssociation	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::TrafficMirrorFilter	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::TrafficMirrorSession	はい	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::TrafficMirrorTarget	はい	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::TransitGateway	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::TransitGatewayAttachment	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::TransitGatewayConnect	はい	いいえ	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::TransitGatewayMulticastDomain	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::TransitGatewayRouteTable	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::VPC	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCBlockPublicAccessExclusion	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::VPCBlockPublicAccessOptions	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EC2::VPCEndpoint	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::VPCEndpointConnectionNotification	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::EC2::VPCEndpointService	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPCPeeringConnection	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPNConnection	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::VPNConnectionRoute	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EC2::VPNGateway	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EC2::Volume	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECR::PullThroughCacheRule	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ECR::RegistryPolicy	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ECR::Repository	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::ECS::CapacityProvider	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ECS::Cluster	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::Service	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::TaskDefinition	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ECS::TaskSet	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EFS::AccessPoint	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EFS::FileSystem	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EKS::Addon	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EKS::Cluster	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::EKS::FargateProfile	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EKS::IdentityProviderConfig	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EMR::SecurityConfiguration	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ElasticBeanstalk::Application	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::ElasticBeanstalk::ApplicationVersion	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ElasticBeanstalk::Environment	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ElasticLoadBalancing::LoadBalancer	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::ElasticLoadBalancingV2::Listener	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ElasticLoadBalancingV2::LoadBalancer	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Elasticsearch::Domain	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::EventSchemas::Discoverer	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EventSchemas::Registry	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EventSchemas::RegistryPolicy	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::EventSchemas::Schema	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Events::ApiDestination	はい	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Events::Archive	はい	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Events::Connection	はい	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Events::Endpoint	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Events::EventBus	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Events::Rule	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Evidently::Launch	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::Evidently::Project	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Evidently::Segment	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::FIS::ExperimentTemplate	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Forecast::Dataset	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Forecast::DatasetGroup	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::FraudDetector::EntityType	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	いいえ
AWS::FraudDetector::Label	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	いいえ
AWS::FraudDetector::Outcome	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	いいえ
AWS::FraudDetector::Variable	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	いいえ

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Glue::Classifier	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Glue::Job	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Glue::MLTransform	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Grafana::Workspace	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::GreengrassV2::ComponentVersion	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::GroundStation::Config	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	いいえ
AWS::GroundStation::DataflowEndpointGroup	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	いいえ
AWS::GroundStation::MissionProfile	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	いいえ

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::GuardDuty::Detector	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::GuardDuty::Filter	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::GuardDuty::IPSet	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::GuardDuty::ThreatIntelSet	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::HealthLake::FHIRDatastore	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
AWS::IAM::Group	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::IAM::Policy	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::IAM::Role	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::IAM::User	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::IVS::Channel	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ	はい
AWS::IVS::PlaybackKeyPair	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ	はい
AWS::IVS::RecordingConfiguration	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::ImageBuilder::ContainerRecipe	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ImageBuilder::DistributionConfiguration	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ImageBuilder::ImagePipeline	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ImageBuilder::ImageRecipe	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::ImageBuilder::InfrastructureConfiguration	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::InspectorV2::Activation	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::InspectorV2::Filter	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::AccountAuditConfiguration	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::IoT::Authorizer	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::CACertificate	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::CustomMetric	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::Dimension	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::IoT::FleetMetric	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::JobTemplate	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::MitigationAction	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::Policy	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::IoT::ProvisioningTemplate	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::RoleAlias	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::ScheduledAudit	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoT::SecurityProfile	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::IoTAnalytics::Channel	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい
AWS::IoTAnalytics::Dataset	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい
AWS::IoTAnalytics::Datastore	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい
AWS::IoTAnalytics::Pipeline	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::IoTEvents::AlarmModel	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoTEvents::DetectorModel	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoTEvents::Input	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoTSiteWise::AssetModel	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::IoTSiteWise::Dashboard	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoTSiteWise::Gateway	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoTSiteWise::Portal	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoTSiteWise::Project	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::IoTTwinMaker::ComponentType	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoTTwinMaker::Entity	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	いいえ
AWS::IoTTwinMaker::Scene	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::IoTTwinMaker::SyncJob	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::IoTTwinMaker::Workspace	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS:: IoTWireless:: FuotaTask	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい
AWS::IoTWireless::MulticastGroup	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい
AWS::IoTWireless::ServiceProfile	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::KMS::Alias	はい	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::KMS::Key	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::KafkaConnect::Connector	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Kendra::Index	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::Kinesis::Stream	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Kinesis::StreamConsumer	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::KinesisAnalyticsV2::Application	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::KinesisFirehose::DeliveryStream	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::KinesisVideo::SignalingChannel	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::KinesisVideo::Stream	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Lambda::CodeSigningConfig	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Lambda::Function	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Lex::Bot	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Lex::BotAlias	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Lightsail::Bucket	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Lightsail::Certificate	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Lightsail::Disk	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Lightsail::StaticIp	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Logs::Destination	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::LookoutMetrics::Alert	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::LookoutVision::Project	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	はい
AWS::M2::Environment	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::MSK::BatchScramSecret	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::MSK::Cluster	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::MSK::ClusterPolicy	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::MSK::Configuration	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::MSK::VpcConnection	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Macie::Session	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::MediaConnect::FlowEntitlement	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::MediaConnect::FlowSource	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::MediaConnect::FlowVpcInterface	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::MediaConnect::Gateway	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::MediaPackage::PackagingConfiguration	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::MediaPackage::PackagingGroup	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::MediaTailor::PlaybackConfiguration	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::MemoryDB::SubnetGroup	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::NetworkFirewall::Firewall	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::NetworkFirewall::FirewallPolicy	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::NetworkFirewall::RuleGroup	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::NetworkFirewall::TLSInspectionConfiguration	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::NetworkFirewall::VpcEndpointAssociation	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::OpenSearch::Domain	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::OpenSearchServerless::Collection	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::OpenSearchServerless::VpcEndpoint	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::Panorama::Package	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	いいえ
AWS::Personalize::Dataset	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Personalize::DatasetGroup	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Personalize::Schema	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Personalize::Solution	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Pinpoint::App	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Pinpoint::ApplicationSettings	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Pinpoint::Campaign	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Pinpoint::EmailChannel	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Pinpoint::EmailTemplate	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Pinpoint::EventStream	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Pinpoint::InAppTemplate	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Pinpoint::Segment	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::QLDB::Ledger	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::QuickSight::DataSource	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::QuickSight::Template	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::QuickSight::Theme	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::RDS::DBCluster	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBClusterSnapshot	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::RDS::DBInstance	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBSecurityGroup	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBSnapshot	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::DBSubnetGroup	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::EventSubscription	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::RDS::GlobalCluster	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::RDS::OptionGroup	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::RUM::AppMonitor	いいえ	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Redshift::Cluster	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterParameterGroup	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterSecurityGroup	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Redshift::ClusterSnapshot	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::ClusterSubnetGroup	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::Redshift::EndpointAccess	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Redshift::EndpointAuthorization	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::Redshift::EventSubscription	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Redshift::ScheduledAction	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::ResilienceHub::App	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::ResilienceHub::ResiliencyPolicy	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::ResourceExplorer2::Index	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::RoboMaker::RobotApplication	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	はい
AWS::RoboMaker::RobotApplicationVersion	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	はい
AWS::RoboMaker::SimulationApplication	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	はい
AWS::Route53Profiles::Profile	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Route53Resolver::FirewallDomainList	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Route53Resolver::FirewallRuleGroup	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Route53Resolver::FirewallRuleGroupAssociation	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Route53Resolver::ResolverEndpoint	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Route53Resolver::ResolverQueryLoggingConfig	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Route53Resolver::ResolverRule	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Route53Resolver::ResolverRuleAssociation	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::S3::AccessPoint	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::S3::AccountPublicAccessBlock	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::S3::Bucket	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::S3::StorageLens	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::S3::StorageLensGroup	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::S3Express::BucketPolicy	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい
AWS::S3Express::DirectoryBucket	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい
AWS::SES::ConfigurationSet	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SES::ContactList	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::SES::ReceiptFilter	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::SES::ReceiptRuleSet	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ	はい
AWS::SES::Template	いいえ	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SNS::Topic	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SQS::Queue	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::SSM::AssociationCompliance	はい	はい	はい	はい	はい	はい	いいえ	はい	はい	はい	いいえ	はい	はい
AWS::SSM::Document	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SSM::FileData	はい	はい	はい	はい	はい	はい	いいえ	はい	はい	はい	いいえ	はい	はい
AWS::SSM::ManagedInstanceInventory	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::SSM::PatchCompliance	はい	はい	はい	はい	はい	はい	いいえ	はい	はい	はい	いいえ	はい	はい
AWS::SageMaker::AppImageConfig	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SageMaker::CodeRepository	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SageMaker::Domain	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::SageMaker::EndpointConfig	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SageMaker::FeatureGroup	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SageMaker::Image	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SageMaker::InferenceExperiment	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::SageMaker::Model	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SageMaker::NotebookInstance	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SageMaker::NotebookInstanceLifecycleConfig	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::SageMaker::Workteam	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::SecretsManager::Secret	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
AWS::SecurityHub::Standard	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::ServiceCatalog::CloudFormationProduct	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ServiceCatalog::CloudFormationProvisionedProduct	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::ServiceCatalog::Portfolio	はい	はい	いいえ	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ServiceDiscovery::HttpNamespace	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ServiceDiscovery::Instance	はい	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::ServiceDiscovery::PublicDnsNamespace	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::ServiceDiscovery::Service	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::ShieldRegional::Protection	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Signer::SigningProfile	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::StepFunctions::Activity	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Step Functions::StateMachine	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Transfer::Agreement	はい	いいえ	はい	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Transfer::Certificate	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Transfer::Connector	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::Transfer::Profile	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::Transfer::Workflow	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::WAFRegional::RateBasedRule	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::WAFRegional::Rule	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::WAFRegional::RuleGroup	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::WAFRegional::WebACL	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい
AWS::WAFv2::IPSet	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::WAFv2::ManagedRuleSet	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::WAFv2::RegexPatternSet	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::WAFv2::RuleGroup	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::WAFv2::WebACL	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい
AWS::WorkSpaces::ConnectionAlias	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	はい

リソースタイプ	アジアパシフィック(香港)	アジアパシフィック(ハイデラバード)	アジアパシフィック(ジャカルタ)	アジアパシフィック(マレーシア)	アジアパシフィック(メルボルン)	アジアパシフィック(ムンバイ)	アジアパシフィック(大阪)	アジアパシフィック(ソウル)	アジアパシフィック(シンガポール)	アジアパシフィック(シドニー)	アジアパシフィック(台北)	アジアパシフィック(タイ)	アジアパシフィック(東京)
AWS::WorkSpaces::Workspace	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ	はい
AWS::XRay::EncryptionConfig	はい	はい	はい	いいえ	はい	はい	はい	はい	はい	はい	いいえ	いいえ	はい

中国リージョン

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::ACM::Certificate	はい	はい
AWS::AmazonMQ::Broker	はい	はい
AWS::ApiGateway::RestApi	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::ApiGateway::Stage	はい	はい
AWS::ApiGatewayV2::Api	はい	はい
AWS::ApiGatewayV2::Stage	はい	はい
AWS::AppConfig::Application	はい	はい
AWS::AppConfig::ConfigurationProfile	はい	はい
AWS::AppConfig::DeploymentStrategy	はい	はい
AWS::AppConfig::Environment	はい	はい
AWS::AppConfig::ExtensionAssociation	はい	はい
AWS::AppConfig::HostedConfigurationVersion	はい	はい
AWS::AppSync::ApiCache	はい	はい
AWS::AppSync::GraphQLApi	はい	はい
AWS::Athena::DataCatalog	はい	はい
AWS::Athena::PreparedStatement	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::Athena::WorkGroup	はい	はい
AWS::AutoScaling::AutoScalingGroup	はい	はい
AWS::AutoScaling::LaunchConfiguration	はい	はい
AWS::AutoScaling::ScalingPolicy	はい	はい
AWS::AutoScaling::ScheduledAction	はい	はい
AWS::AutoScaling::WarmPool	はい	はい
AWS::Backup::BackupPlan	はい	はい
AWS::Backup::BackupSelection	はい	はい
AWS::Backup::BackupVault	はい	はい
AWS::Backup::RecoveryPoint	はい	はい
AWS::Batch::ComputeEnvironment	はい	はい
AWS::Batch::JobQueue	はい	はい
AWS::Batch::SchedulingPolicy	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::Cassandra::Keyspace	はい	はい
AWS::CloudFormation::Stack	はい	はい
AWS::CloudTrail::Trail	はい	はい
AWS::CloudWatch::Alarm	はい	はい
AWS::CloudWatch::MetricStream	はい	はい
AWS::CodeBuild::Project	はい	はい
AWS::CodeBuild::ReportGroup	はい	はい
AWS::Cognito::IdentityPool	はい	いいえ
AWS::Config::ConfigurationRecorder	はい	はい
AWS::Config::ResourceCompliance	はい	はい
AWS::DMS::Certificate	はい	はい
AWS::DMS::Endpoint	はい	はい
AWS::DMS::EventSubscription	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::DMS::ReplicationInstance	はい	はい
AWS::DMS::ReplicationSubnetGroup	はい	はい
AWS::DMS::ReplicationTask	はい	はい
AWS::DataSync::LocationEFS	はい	はい
AWS::DataSync::LocationHDFS	はい	はい
AWS::DataSync::LocationNFS	はい	はい
AWS::DataSync::LocationObjectStorage	はい	はい
AWS::DataSync::LocationS3	はい	はい
AWS::DataSync::LocationSMB	はい	はい
AWS::DataSync::Task	はい	はい
AWS::DynamoDB::Table	はい	はい
AWS::EC2::CapacityReservation	はい	はい
AWS::EC2::DHCPOptions	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::EC2::EC2Fleet	はい	はい
AWS::EC2::EIP	はい	はい
AWS::EC2::EIPAssociation	はい	はい
AWS::EC2::FlowLog	はい	はい
AWS::EC2::Host	はい	はい
AWS::EC2::Instance	はい	はい
AWS::EC2::InternetGateway	はい	はい
AWS::EC2::LaunchTemplate	はい	はい
AWS::EC2::NatGateway	はい	はい
AWS::EC2::NetworkAcl	はい	はい
AWS::EC2::NetworkInterface	はい	はい
AWS::EC2::PrefixList	はい	はい
AWS::EC2::RouteTable	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::EC2::SecurityGroup	はい	はい
AWS::EC2::SnapshotBlockPublicAccess	はい	はい
AWS::EC2::SpotFleet	はい	はい
AWS::EC2::Subnet	はい	はい
AWS::EC2::SubnetRouteTableAssociation	はい	はい
AWS::EC2::TrafficMirrorFilter	はい	はい
AWS::EC2::TrafficMirrorSession	はい	はい
AWS::EC2::TrafficMirrorTarget	はい	はい
AWS::EC2::TransitGateway	はい	はい
AWS::EC2::TransitGatewayAttachment	はい	はい
AWS::EC2::TransitGatewayConnect	はい	はい
AWS::EC2::TransitGatewayMulticastDomain	はい	はい
AWS::EC2::TransitGatewayRouteTable	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::EC2::VPC	はい	はい
AWS::EC2::VPCBlockPublicAccessExclusion	はい	はい
AWS::EC2::VPCBlockPublicAccessOptions	はい	はい
AWS::EC2::VPCEndpoint	はい	はい
AWS::EC2::VPCEndpointConnectionNotification	はい	はい
AWS::EC2::VPCEndpointService	はい	はい
AWS::EC2::VPCPeeringConnection	はい	はい
AWS::EC2::VPNGateway	はい	いいえ
AWS::EC2::Volume	はい	はい
AWS::ECR::Repository	はい	はい
AWS::ECS::CapacityProvider	はい	はい
AWS::ECS::Cluster	はい	はい
AWS::ECS::Service	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::ECS::TaskDefinition	はい	はい
AWS::ECS::TaskSet	はい	はい
AWS::EFS::AccessPoint	はい	はい
AWS::EFS::FileSystem	はい	はい
AWS::EKS::Addon	はい	はい
AWS::EKS::Cluster	はい	はい
AWS::EKS::FargateProfile	はい	はい
AWS::EKS::IdentityProviderConfig	はい	はい
AWS::EMR::SecurityConfiguration	はい	はい
AWS::ElasticBeanstalk::Application	はい	はい
AWS::ElasticBeanstalk::ApplicationVersion	はい	はい
AWS::ElasticBeanstalk::Environment	はい	はい
AWS::ElasticLoadBalancing::LoadBalancer	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::ElasticLoadBalancingV2::Listener	はい	はい
AWS::ElasticLoadBalancingV2::LoadBalancer	はい	はい
AWS::Elasticsearch::Domain	はい	はい
AWS::Events::Archive	はい	はい
AWS::Events::EventBus	はい	はい
AWS::Events::Rule	はい	はい
AWS::Glue::Classifier	はい	はい
AWS::Glue::Job	はい	はい
AWS::Glue::MLTransform	はい	いいえ
AWS::GreengrassV2::ComponentVersion	はい	いいえ
AWS::GuardDuty::Filter	はい	はい
AWS::GuardDuty::ThreatIntelSet	はい	はい
AWS::IAM::Group	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::IAM::InstanceProfile	はい	いいえ
AWS::IAM::OIDCProvider	はい	いいえ
AWS::IAM::Policy	はい	はい
AWS::IAM::Role	はい	はい
AWS::IAM::SAMLProvider	はい	いいえ
AWS::IAM::ServerCertificate	はい	いいえ
AWS::IAM::User	はい	はい
AWS::ImageBuilder::ContainerRecipe	はい	はい
AWS::ImageBuilder::DistributionConfiguration	はい	はい
AWS::ImageBuilder::ImagePipeline	はい	はい
AWS::ImageBuilder::ImageRecipe	はい	はい
AWS::ImageBuilder::InfrastructureConfiguration	はい	はい
AWS::InspectorV2::Activation	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::IoT::AccountAuditConfiguration	はい	はい
AWS::IoT::Authorizer	はい	はい
AWS::IoT::CACertificate	はい	はい
AWS::IoT::CustomMetric	はい	はい
AWS::IoT::Dimension	はい	はい
AWS::IoT::FleetMetric	はい	はい
AWS::IoT::JobTemplate	はい	はい
AWS::IoT::MitigationAction	はい	はい
AWS::IoT::Policy	はい	はい
AWS::IoT::ProvisioningTemplate	はい	はい
AWS::IoT::RoleAlias	はい	はい
AWS::IoT::ScheduledAudit	はい	はい
AWS::IoT::SecurityProfile	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::IoTAnalytics::Channel	はい	いいえ
AWS::IoTAnalytics::Dataset	はい	いいえ
AWS::IoTAnalytics::Datastore	はい	いいえ
AWS::IoTAnalytics::Pipeline	はい	いいえ
AWS::IoTEvents::AlarmModel	はい	いいえ
AWS::IoTEvents::DetectorModel	はい	いいえ
AWS::IoTEvents::Input	はい	いいえ
AWS::IoTSiteWise::AssetModel	はい	いいえ
AWS::IoTSiteWise::Dashboard	はい	いいえ
AWS::IoTSiteWise::Gateway	はい	いいえ
AWS::IoTSiteWise::Portal	はい	いいえ
AWS::IoTSiteWise::Project	はい	いいえ
AWS::KMS::Alias	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::KMS::Key	はい	はい
AWS::Kinesis::Stream	はい	はい
AWS::Kinesis::StreamConsumer	はい	はい
AWS::KinesisAnalyticsV2::Application	はい	はい
AWS::KinesisFirehose::DeliveryStream	はい	はい
AWS::Lambda::Function	はい	いいえ
AWS::Logs::Destination	はい	はい
AWS::MSK::BatchScramSecret	はい	はい
AWS::MSK::Cluster	はい	はい
AWS::MSK::ClusterPolicy	はい	はい
AWS::MSK::Configuration	はい	はい
AWS::MSK::VpcConnection	はい	はい
AWS::NetworkFirewall::Firewall	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::NetworkFirewall::FirewallPolicy	はい	はい
AWS::NetworkFirewall::RuleGroup	はい	はい
AWS::NetworkFirewall::TLSInspectionConfiguration	はい	はい
AWS::NetworkFirewall::VpcEndpointAssociation	はい	はい
AWS::OpenSearch::Domain	はい	はい
AWS::Personalize::Dataset	はい	いいえ
AWS::Personalize::DatasetGroup	はい	いいえ
AWS::Personalize::Schema	はい	いいえ
AWS::Personalize::Solution	はい	いいえ
AWS::RDS::DBCluster	いいえ	はい
AWS::RDS::DBClusterSnapshot	はい	はい
AWS::RDS::DBInstance	はい	はい
AWS::RDS::DBSecurityGroup	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::RDS::DBSnapshot	はい	はい
AWS::RDS::DBSubnetGroup	はい	はい
AWS::RDS::EventSubscription	はい	はい
AWS::RDS::OptionGroup	はい	はい
AWS::Redshift::Cluster	はい	はい
AWS::Redshift::ClusterParameterGroup	はい	はい
AWS::Redshift::ClusterSecurityGroup	はい	はい
AWS::Redshift::ClusterSnapshot	はい	はい
AWS::Redshift::ClusterSubnetGroup	はい	はい
AWS::Redshift::EventSubscription	はい	はい
AWS::Route53Profiles::Profile	はい	はい
AWS::Route53Resolver::FirewallDomainList	はい	はい
AWS::Route53Resolver::FirewallRuleGroupAssociation	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::Route53Resolver::ResolverEndpoint	はい	はい
AWS::Route53Resolver::ResolverQueryLoggingConfig	はい	はい
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	はい	はい
AWS::Route53Resolver::ResolverRule	はい	はい
AWS::Route53Resolver::ResolverRuleAssociation	はい	はい
AWS::S3::AccessPoint	はい	はい
AWS::S3::AccountPublicAccessBlock	はい	はい
AWS::S3::Bucket	はい	はい
AWS::S3::StorageLensGroup	はい	はい
AWS::SES::ConfigurationSet	いいえ	はい
AWS::SES::ContactList	いいえ	はい
AWS::SES::Template	いいえ	はい
AWS::SNS::Topic	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::SQS::Queue	はい	はい
AWS::SSM::AssociationCompliance	はい	はい
AWS::SSM::Document	はい	はい
AWS::SSM::FileData	はい	はい
AWS::SSM::ManagedInstanceInventory	はい	はい
AWS::SSM::PatchCompliance	はい	はい
AWS::SageMaker::AppImageConfig	はい	はい
AWS::SageMaker::CodeRepository	はい	はい
AWS::SageMaker::Domain	はい	はい
AWS::SageMaker::EndpointConfig	はい	はい
AWS::SageMaker::FeatureGroup	はい	はい
AWS::SageMaker::Image	はい	はい
AWS::SageMaker::Model	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::SageMaker::NotebookInstance	はい	はい
AWS::SageMaker::NotebookInstanceLifecycleConfig	はい	はい
AWS::SecretsManager::Secret	はい	はい
AWS::SecurityHub::Standard	はい	はい
AWS::ServiceCatalog::CloudFormationProduct	はい	はい
AWS::ServiceCatalog::CloudFormationProvisionedProduct	はい	はい
AWS::ServiceCatalog::Portfolio	はい	はい
AWS::ServiceDiscovery::HttpNamespace	はい	はい
AWS::ServiceDiscovery::Instance	はい	はい
AWS::ServiceDiscovery::PublicDnsNamespace	はい	はい
AWS::ServiceDiscovery::Service	はい	はい
AWS::StepFunctions::Activity	はい	いいえ
AWS::StepFunctions::StateMachine	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::Transfer::Agreement	はい	はい
AWS::Transfer::Certificate	はい	はい
AWS::Transfer::Connector	はい	はい
AWS::Transfer::Profile	はい	はい
AWS::Transfer::Workflow	はい	はい
AWS::WAFRegional::RateBasedRule	はい	はい
AWS::WAFRegional::Rule	はい	はい
AWS::WAFRegional::RuleGroup	はい	はい
AWS::WAFRegional::WebACL	はい	はい
AWS::WAFv2::IPSet	はい	はい
AWS::WAFv2::ManagedRuleSet	はい	はい
AWS::WAFv2::RegexPatternSet	はい	はい
AWS::WAFv2::RuleGroup	はい	はい

リソースタイプ	中国 (北京)	中国 (寧夏)
AWS::WAFv2::WebACL	はい	はい
AWS::WorkSpaces::Workspace	いいえ	はい

アフリカおよび中東リージョン

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::ACM::Certificate	はい	はい	はい	はい
AWS::ACMPCA::CertificateAuthority	はい	はい	はい	はい
AWS::ACMPCA::CertificateAuthorityActivation	はい	はい	はい	はい
AWS::AccessAnalyzer::Analyzer	はい	はい	はい	はい
AWS::AmazonMQ::Broker	はい	いいえ	はい	はい
AWS::Amplify::App	いいえ	いいえ	はい	いいえ
AWS::Amplify::Branch	いいえ	いいえ	はい	いいえ
AWS::ApiGateway::RestApi	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::ApiGateway::Stage	はい	はい	はい	はい
AWS::ApiGatewayV2::Api	はい	はい	はい	はい
AWS::ApiGatewayV2::Stage	はい	はい	はい	はい
AWS::AppConfig::Application	はい	はい	はい	いいえ
AWS::AppConfig::ConfigurationProfile	はい	はい	はい	いいえ
AWS::AppConfig::DeploymentStrategy	はい	はい	はい	はい
AWS::AppConfig::Environment	はい	はい	はい	いいえ
AWS::AppConfig::ExtensionAssociation	はい	はい	はい	はい
AWS::AppConfig::HostedConfigurationVersion	はい	はい	はい	いいえ
AWS::AppFlow::Flow	はい	いいえ	いいえ	いいえ
AWS::AppIntegrations::Application	はい	いいえ	いいえ	いいえ
AWS::AppIntegrations::EventIntegration	はい	いいえ	いいえ	いいえ

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::AppMesh::GatewayRoute	はい	はい	はい	いいえ
AWS::AppMesh::Mesh	はい	はい	はい	いいえ
AWS::AppMesh::Route	はい	はい	はい	いいえ
AWS::AppMesh::VirtualGateway	はい	はい	はい	いいえ
AWS::AppMesh::VirtualNode	はい	はい	はい	いいえ
AWS::AppMesh::VirtualRouter	はい	はい	はい	いいえ
AWS::AppMesh::VirtualService	はい	はい	はい	いいえ
AWS::AppSync::ApiCache	はい	はい	はい	はい
AWS::AppSync::GraphQLApi	はい	はい	はい	はい
AWS::Athena::DataCatalog	はい	はい	はい	はい
AWS::Athena::PreparedStatement	はい	はい	はい	はい
AWS::Athena::WorkGroup	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::AutoScaling::AutoScalingGroup	はい	はい	はい	はい
AWS::AutoScaling::LaunchConfiguration	はい	はい	はい	はい
AWS::AutoScaling::ScalingPolicy	はい	はい	はい	はい
AWS::AutoScaling::ScheduledAction	はい	はい	はい	はい
AWS::AutoScaling::WarmPool	はい	いいえ	はい	いいえ
AWS::Backup::BackupPlan	はい	はい	はい	はい
AWS::Backup::BackupSelection	はい	はい	はい	はい
AWS::Backup::BackupVault	はい	はい	はい	はい
AWS::Backup::RecoveryPoint	はい	はい	はい	はい
AWS::Backup::ReportPlan	はい	いいえ	はい	いいえ
AWS::Batch::ComputeEnvironment	はい	いいえ	はい	はい
AWS::Batch::JobQueue	はい	いいえ	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::Batch::SchedulingPolicy	はい	はい	はい	はい
AWS::Cassandra::Keyspace	いいえ	いいえ	はい	いいえ
AWS::Cloud9::EnvironmentEC2	はい	いいえ	はい	いいえ
AWS::CloudFormation::Stack	はい	いいえ	はい	いいえ
AWS::CloudTrail::Trail	はい	はい	はい	はい
AWS::CloudWatch::Alarm	はい	はい	はい	はい
AWS::CloudWatch::MetricStream	はい	はい	はい	はい
AWS::CodeBuild::Project	はい	はい	はい	はい
AWS::CodeBuild::ReportGroup	はい	はい	はい	はい
AWS::CodeDeploy::Application	はい	いいえ	はい	いいえ
AWS::CodeDeploy::DeploymentConfig	はい	いいえ	はい	いいえ
AWS::CodeDeploy::DeploymentGroup	はい	いいえ	はい	いいえ

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::CodePipeline::Pipeline	いいえ	はい	いいえ	はい
AWS::Cognito::IdentityPool	はい	はい	はい	はい
AWS::Cognito::UserPool	はい	はい	はい	はい
AWS::Cognito::UserPoolClient	はい	はい	はい	はい
AWS::Cognito::UserPoolGroup	はい	はい	はい	はい
AWS::Config::ConfigurationRecorder	はい	はい	はい	はい
AWS::Config::ConformancePackCompliance	はい	はい	はい	はい
AWS::Config::ResourceCompliance	はい	はい	はい	はい
AWS::Connect::Instance	はい	いいえ	いいえ	いいえ
AWS::Connect::PhoneNumber	はい	いいえ	いいえ	いいえ
AWS::Connect::QuickConnect	はい	いいえ	いいえ	いいえ
AWS::Connect::Rule	はい	いいえ	いいえ	いいえ

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::Connect::User	はい	いいえ	いいえ	いいえ
AWS::CustomerProfiles::Domain	はい	いいえ	いいえ	いいえ
AWS::CustomerProfiles::ObjectType	はい	いいえ	いいえ	いいえ
AWS::DMS::Certificate	はい	いいえ	はい	いいえ
AWS::DMS::Endpoint	はい	いいえ	はい	いいえ
AWS::DMS::EventSubscription	はい	いいえ	はい	いいえ
AWS::DMS::ReplicationInstance	はい	いいえ	はい	いいえ
AWS::DMS::ReplicationSubnetGroup	はい	いいえ	はい	いいえ
AWS::DMS::ReplicationTask	はい	いいえ	はい	いいえ
AWS::DataSync::LocationEFS	はい	いいえ	はい	はい
AWS::DataSync::LocationFSxLustre	はい	いいえ	はい	いいえ
AWS::DataSync::LocationFSxWindows	はい	いいえ	はい	いいえ

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::DataSync::LocationHDFS	はい	いいえ	はい	はい
AWS::DataSync::LocationNFS	はい	いいえ	はい	はい
AWS::DataSync::LocationObjectStorage	はい	いいえ	はい	はい
AWS::DataSync::LocationS3	はい	はい	はい	はい
AWS::DataSync::LocationSMB	はい	いいえ	はい	はい
AWS::DataSync::Task	はい	はい	はい	はい
AWS::Detective::Graph	はい	はい	はい	いいえ
AWS::DynamoDB::Table	はい	はい	はい	はい
AWS::EC2::CapacityReservation	はい	はい	はい	はい
AWS::EC2::ClientVpnEndpoint	はい	いいえ	はい	いいえ
AWS::EC2::ClientVpnTargetNetworkAssociation	はい	はい	はい	いいえ
AWS::EC2::CustomerGateway	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::EC2::DHCPOptions	はい	はい	はい	はい
AWS::EC2::EC2Fleet	はい	いいえ	はい	はい
AWS::EC2::EIP	はい	はい	はい	はい
AWS::EC2::EIPAssociation	はい	はい	はい	はい
AWS::EC2::EgressOnlyInternetGateway	はい	いいえ	はい	はい
AWS::EC2::FlowLog	はい	いいえ	はい	はい
AWS::EC2::Host	はい	はい	はい	はい
AWS::EC2::IPAM	はい	いいえ	はい	はい
AWS::EC2::IPAMPool	はい	いいえ	はい	はい
AWS::EC2::IPAMResourceDiscovery	はい	はい	はい	はい
AWS::EC2::IPAMResourceDiscoveryAssociation	はい	はい	はい	はい
AWS::EC2::IPAMScope	はい	いいえ	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::EC2::Instance	はい	はい	はい	はい
AWS::EC2::InstanceConnectEndpoint	はい	はい	はい	はい
AWS::EC2::InternetGateway	はい	はい	はい	はい
AWS::EC2::LaunchTemplate	はい	いいえ	はい	いいえ
AWS::EC2::NatGateway	はい	いいえ	はい	はい
AWS::EC2::NetworkAcl	はい	はい	はい	はい
AWS::EC2::NetworkInsightsAccessScope	はい	いいえ	はい	いいえ
AWS::EC2::NetworkInsightsAccessScopeAnalysis	はい	いいえ	はい	いいえ
AWS::EC2::NetworkInsightsAnalysis	はい	いいえ	はい	いいえ
AWS::EC2::NetworkInsightsPath	はい	いいえ	はい	いいえ
AWS::EC2::NetworkInterface	はい	はい	はい	はい
AWS::EC2::PrefixList	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::EC2::RouteTable	はい	はい	はい	はい
AWS::EC2::SecurityGroup	はい	はい	はい	はい
AWS::EC2::SnapshotBlockPublicAccess	はい	はい	はい	はい
AWS::EC2::SpotFleet	はい	はい	はい	はい
AWS::EC2::Subnet	はい	はい	はい	はい
AWS::EC2::SubnetRouteTableAssociation	はい	はい	はい	はい
AWS::EC2::TrafficMirrorFilter	はい	はい	はい	はい
AWS::EC2::TrafficMirrorSession	いいえ	いいえ	はい	いいえ
AWS::EC2::TrafficMirrorTarget	いいえ	いいえ	はい	いいえ
AWS::EC2::TransitGateway	はい	はい	はい	はい
AWS::EC2::TransitGatewayAttachment	はい	いいえ	はい	はい
AWS::EC2::TransitGatewayConnect	はい	いいえ	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::EC2::TransitGatewayMulticastDomain	はい	はい	はい	はい
AWS::EC2::TransitGatewayRouteTable	はい	いいえ	はい	はい
AWS::EC2::VPC	はい	はい	はい	はい
AWS::EC2::VPCBlockPublicAccessExclusion	はい	はい	はい	はい
AWS::EC2::VPCBlockPublicAccessOptions	はい	はい	はい	はい
AWS::EC2::VPCEndpoint	はい	はい	はい	はい
AWS::EC2::VPCEndpointConnectionNotification	はい	はい	はい	はい
AWS::EC2::VPCEndpointService	はい	はい	はい	はい
AWS::EC2::VPCPeeringConnection	はい	はい	はい	はい
AWS::EC2::VPNConnection	はい	はい	はい	はい
AWS::EC2::VPNConnectionRoute	はい	はい	はい	はい
AWS::EC2::VPNGateway	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::EC2::Volume	はい	はい	はい	はい
AWS::ECR::PullThroughCacheRule	はい	はい	はい	はい
AWS::ECR::RegistryPolicy	はい	はい	はい	はい
AWS::ECR::Repository	はい	はい	はい	はい
AWS::ECS::CapacityProvider	はい	はい	はい	はい
AWS::ECS::Cluster	はい	はい	はい	はい
AWS::ECS::Service	はい	はい	はい	はい
AWS::ECS::TaskDefinition	はい	はい	はい	はい
AWS::ECS::TaskSet	はい	いいえ	はい	はい
AWS::EFS::AccessPoint	はい	はい	はい	はい
AWS::EFS::FileSystem	はい	はい	はい	はい
AWS::EKS::Addon	はい	いいえ	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::EKS::Cluster	はい	いいえ	はい	はい
AWS::EKS::FargateProfile	はい	はい	はい	はい
AWS::EKS::IdentityProviderConfig	はい	いいえ	はい	はい
AWS::EMR::SecurityConfiguration	はい	はい	はい	はい
AWS::ElasticBeanstalk::Application	はい	いいえ	はい	はい
AWS::ElasticBeanstalk::ApplicationVersion	はい	いいえ	はい	はい
AWS::ElasticBeanstalk::Environment	はい	いいえ	はい	はい
AWS::ElasticLoadBalancing::LoadBalancer	はい	はい	はい	はい
AWS::ElasticLoadBalancingV2::Listener	はい	いいえ	はい	いいえ
AWS::ElasticLoadBalancingV2::LoadBalancer	はい	はい	はい	はい
AWS::Elasticsearch::Domain	はい	はい	はい	はい
AWS::EventSchemas::Discoverer	はい	いいえ	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::EventSchemas::Registry	はい	いいえ	はい	はい
AWS::EventSchemas::RegistryPolicy	はい	いいえ	はい	はい
AWS::EventSchemas::Schema	はい	いいえ	はい	はい
AWS::Events::ApiDestination	はい	いいえ	はい	はい
AWS::Events::Archive	はい	いいえ	はい	はい
AWS::Events::Connection	はい	いいえ	はい	はい
AWS::Events::EventBus	はい	はい	はい	はい
AWS::Events::Rule	はい	いいえ	はい	いいえ
AWS::FIS::ExperimentTemplate	はい	いいえ	はい	いいえ
AWS::Glue::Classifier	はい	はい	はい	はい
AWS::Glue::Job	はい	はい	はい	はい
AWS::Glue::MLTransform	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::GroundStation::Config	はい	いいえ	はい	いいえ
AWS::GroundStation::DataflowEndpointGroup	はい	いいえ	はい	いいえ
AWS::GroundStation::MissionProfile	はい	いいえ	はい	いいえ
AWS::GuardDuty::Detector	はい	はい	はい	はい
AWS::GuardDuty::Filter	はい	いいえ	はい	いいえ
AWS::GuardDuty::IPSet	はい	いいえ	はい	はい
AWS::GuardDuty::ThreatIntelSet	はい	はい	はい	はい
AWS::IAM::Group	はい	いいえ	はい	いいえ
AWS::IAM::Policy	はい	いいえ	はい	いいえ
AWS::IAM::Role	はい	いいえ	はい	いいえ
AWS::IAM::User	はい	いいえ	はい	いいえ
AWS::ImageBuilder::ContainerRecipe	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::ImageBuilder::DistributionConfiguration	はい	はい	はい	はい
AWS::ImageBuilder::ImagePipeline	はい	はい	はい	はい
AWS::ImageBuilder::ImageRecipe	はい	はい	はい	はい
AWS::ImageBuilder::InfrastructureConfiguration	はい	はい	はい	はい
AWS::InspectorV2::Activation	はい	いいえ	はい	いいえ
AWS::InspectorV2::Filter	はい	いいえ	はい	いいえ
AWS::IoT::AccountAuditConfiguration	いいえ	いいえ	はい	はい
AWS::IoT::Authorizer	いいえ	いいえ	はい	はい
AWS::IoT::CACertificate	いいえ	いいえ	はい	はい
AWS::IoT::CustomMetric	いいえ	いいえ	はい	はい
AWS::IoT::Dimension	いいえ	いいえ	はい	はい
AWS::IoT::FleetMetric	いいえ	いいえ	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::IoT::JobTemplate	いいえ	いいえ	はい	はい
AWS::IoT::MitigationAction	いいえ	いいえ	はい	はい
AWS::IoT::Policy	いいえ	いいえ	はい	はい
AWS::IoT::ProvisioningTemplate	いいえ	いいえ	はい	はい
AWS::IoT::RoleAlias	いいえ	いいえ	はい	はい
AWS::IoT::ScheduledAudit	いいえ	いいえ	はい	はい
AWS::IoT::SecurityProfile	いいえ	いいえ	はい	はい
AWS::KMS::Alias	はい	いいえ	はい	はい
AWS::KMS::Key	はい	はい	はい	はい
AWS::Kinesis::Stream	はい	いいえ	はい	はい
AWS::Kinesis::StreamConsumer	はい	はい	はい	はい
AWS::KinesisAnalyticsV2::Application	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::KinesisFirehose::DeliveryStream	はい	はい	はい	はい
AWS::Lambda::CodeSigningConfig	はい	いいえ	はい	いいえ
AWS::Lambda::Function	はい	はい	はい	はい
AWS::Lex::Bot	はい	いいえ	いいえ	いいえ
AWS::Lex::BotAlias	はい	いいえ	いいえ	いいえ
AWS::Logs::Destination	はい	はい	はい	はい
AWS::MSK::BatchScramSecret	はい	いいえ	はい	はい
AWS::MSK::Cluster	はい	いいえ	はい	はい
AWS::MSK::ClusterPolicy	はい	はい	はい	はい
AWS::MSK::Configuration	はい	はい	はい	はい
AWS::MSK::VpcConnection	はい	はい	はい	はい
AWS::Macie::Session	はい	はい	はい	いいえ

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::MediaConnect::FlowEntitlement	はい	いいえ	いいえ	はい
AWS::MediaConnect::FlowSource	はい	いいえ	いいえ	はい
AWS::MediaConnect::FlowVpcInterface	はい	いいえ	いいえ	いいえ
AWS::MediaConnect::Gateway	はい	いいえ	いいえ	いいえ
AWS::MediaTailor::PlaybackConfiguration	はい	いいえ	いいえ	はい
AWS::NetworkFirewall::Firewall	はい	はい	はい	はい
AWS::NetworkFirewall::FirewallPolicy	はい	はい	はい	はい
AWS::NetworkFirewall::RuleGroup	はい	はい	はい	はい
AWS::NetworkFirewall::TLSInspectionConfiguration	はい	はい	はい	はい
AWS::NetworkFirewall::VpcEndpointAssociation	はい	はい	はい	はい
AWS::OpenSearch::Domain	はい	いいえ	はい	いいえ
AWS::RDS::DBCluster	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::RDS::DBClusterSnapshot	はい	いいえ	はい	はい
AWS::RDS::DBInstance	はい	はい	はい	はい
AWS::RDS::DBSecurityGroup	はい	はい	はい	はい
AWS::RDS::DBSnapshot	はい	はい	はい	はい
AWS::RDS::DBSubnetGroup	はい	はい	はい	はい
AWS::RDS::EventSubscription	はい	はい	はい	はい
AWS::RDS::GlobalCluster	はい	はい	はい	はい
AWS::RDS::OptionGroup	はい	はい	はい	はい
AWS::RUM::AppMonitor	いいえ	いいえ	はい	はい
AWS::Redshift::Cluster	はい	はい	はい	はい
AWS::Redshift::ClusterParameterGroup	はい	はい	はい	はい
AWS::Redshift::ClusterSecurityGroup	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::Redshift::ClusterSnapshot	はい	はい	はい	はい
AWS::Redshift::ClusterSubnetGroup	はい	はい	はい	はい
AWS::Redshift::EventSubscription	はい	はい	はい	はい
AWS::Redshift::ScheduledAction	いいえ	いいえ	はい	いいえ
AWS::ResilienceHub::App	はい	いいえ	はい	いいえ
AWS::ResilienceHub::ResiliencyPolicy	はい	いいえ	はい	いいえ
AWS::ResourceExplorer2::Index	いいえ	いいえ	はい	はい
AWS::Route53Profiles::Profile	はい	はい	はい	はい
AWS::Route53Resolver::FirewallDomainList	はい	いいえ	はい	いいえ
AWS::Route53Resolver::FirewallRuleGroup	はい	いいえ	はい	いいえ
AWS::Route53Resolver::FirewallRuleGroupAssociation	はい	いいえ	はい	いいえ
AWS::Route53Resolver::ResolverEndpoint	はい	いいえ	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::Route53Resolver::ResolverQueryLoggingConfig	はい	いいえ	はい	いいえ
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	はい	いいえ	はい	いいえ
AWS::Route53Resolver::ResolverRule	はい	いいえ	はい	はい
AWS::Route53Resolver::ResolverRuleAssociation	はい	いいえ	はい	はい
AWS::S3::AccessPoint	はい	はい	はい	はい
AWS::S3::AccountPublicAccessBlock	はい	いいえ	はい	はい
AWS::S3::Bucket	はい	はい	はい	はい
AWS::SES::ConfigurationSet	はい	はい	はい	いいえ
AWS::SES::ContactList	はい	はい	はい	いいえ
AWS::SES::Template	はい	はい	はい	いいえ
AWS::SNS::Topic	はい	はい	はい	はい
AWS::SQS::Queue	はい	いいえ	はい	いいえ

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::SSM::AssociationCompliance	はい	はい	はい	はい
AWS::SSM::Document	はい	はい	はい	はい
AWS::SSM::FileData	はい	はい	はい	はい
AWS::SSM::ManagedInstanceInventory	はい	はい	はい	はい
AWS::SSM::PatchCompliance	はい	はい	はい	はい
AWS::SageMaker::AppImageConfig	はい	はい	はい	はい
AWS::SageMaker::CodeRepository	はい	いいえ	はい	いいえ
AWS::SageMaker::Domain	はい	いいえ	はい	いいえ
AWS::SageMaker::EndpointConfig	はい	いいえ	はい	いいえ
AWS::SageMaker::FeatureGroup	はい	はい	はい	いいえ
AWS::SageMaker::Image	はい	はい	はい	はい
AWS::SageMaker::InferenceExperiment	はい	いいえ	はい	いいえ

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::SageMaker::Model	はい	いいえ	はい	いいえ
AWS::SageMaker::NotebookInstance	はい	いいえ	はい	いいえ
AWS::SageMaker::NotebookInstanceLifecycleConfig	はい	いいえ	はい	いいえ
AWS::SecretsManager::Secret	はい	はい	はい	はい
AWS::SecurityHub::Standard	はい	はい	はい	はい
AWS::ServiceCatalog::CloudFormationProduct	はい	いいえ	はい	はい
AWS::ServiceCatalog::CloudFormationProvisionedProduct	はい	いいえ	はい	はい
AWS::ServiceCatalog::Portfolio	はい	いいえ	はい	はい
AWS::ServiceDiscovery::HttpNamespace	はい	はい	はい	はい
AWS::ServiceDiscovery::Instance	はい	いいえ	はい	はい
AWS::ServiceDiscovery::PublicDnsNamespace	はい	はい	はい	はい
AWS::ServiceDiscovery::Service	はい	いいえ	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::ShieldRegional::Protection	はい	いいえ	はい	はい
AWS::Signer::SigningProfile	はい	いいえ	はい	いいえ
AWS::StepFunctions::Activity	はい	はい	はい	はい
AWS::StepFunctions::StateMachine	はい	はい	はい	はい
AWS::Transfer::Agreement	はい	いいえ	はい	はい
AWS::Transfer::Certificate	はい	はい	はい	はい
AWS::Transfer::Connector	はい	はい	はい	はい
AWS::Transfer::Profile	はい	はい	はい	はい
AWS::Transfer::Workflow	はい	はい	はい	はい
AWS::WAFRegional::RateBasedRule	はい	はい	はい	はい
AWS::WAFRegional::Rule	はい	はい	はい	はい
AWS::WAFRegional::RuleGroup	はい	はい	はい	はい

リソースタイプ	アフリカ (ケープタウン)	イスラエル (テルアビブ)	中東 (バーレーン)	中東 (アラブ首長国連邦)
AWS::WAFRegional::WebACL	はい	はい	はい	はい
AWS::WAFv2::IPSet	はい	はい	はい	はい
AWS::WAFv2::ManagedRuleSet	はい	はい	はい	はい
AWS::WAFv2::RegexPatternSet	はい	はい	はい	はい
AWS::WAFv2::RuleGroup	はい	はい	はい	はい
AWS::WAFv2::WebACL	はい	はい	はい	はい
AWS::WorkSpaces::Workspace	はい	いいえ	いいえ	いいえ
AWS::XRay::EncryptionConfig	はい	はい	いいえ	はい

GovCloud リージョン

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::ACM::Certificate	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::ACMPCA::CertificateAuthority	はい	はい
AWS::ACMPCA::CertificateAuthorityActivation	はい	はい
AWS::AccessAnalyzer::Analyzer	はい	はい
AWS::AmazonMQ::Broker	はい	はい
AWS::ApiGateway::RestApi	はい	はい
AWS::ApiGateway::Stage	はい	はい
AWS::ApiGatewayV2::Api	はい	はい
AWS::ApiGatewayV2::Stage	はい	はい
AWS::AppConfig::Application	はい	はい
AWS::AppConfig::ConfigurationProfile	はい	はい
AWS::AppConfig::DeploymentStrategy	はい	はい
AWS::AppConfig::Environment	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::AppConfig::ExtensionAssociation	はい	はい
AWS::AppConfig::HostedConfigurationVersion	はい	はい
AWS::AppStream::Application	はい	はい
AWS::AppStream::DirectoryConfig	はい	いいえ
AWS::AppStream::Fleet	はい	いいえ
AWS::AppStream::Stack	はい	いいえ
AWS::Athena::DataCatalog	はい	はい
AWS::Athena::WorkGroup	はい	はい
AWS::AutoScaling::AutoScalingGroup	はい	はい
AWS::AutoScaling::LaunchConfiguration	はい	はい
AWS::AutoScaling::ScalingPolicy	はい	はい
AWS::AutoScaling::ScheduledAction	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::AutoScaling::WarmPool	はい	はい
AWS::Backup::BackupPlan	はい	はい
AWS::Backup::BackupSelection	はい	はい
AWS::Backup::BackupVault	はい	はい
AWS::Backup::RecoveryPoint	はい	はい
AWS::Batch::ComputeEnvironment	はい	はい
AWS::Batch::JobQueue	はい	はい
AWS::Batch::SchedulingPolicy	はい	はい
AWS::Bedrock::Guardrail	はい	はい
AWS::Bedrock::KnowledgeBase	はい	はい
AWS::Cassandra::Keyspace	はい	はい
AWS::CloudFormation::Stack	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::CloudTrail::Trail	はい	はい
AWS::CloudWatch::Alarm	はい	はい
AWS::CodeBuild::Project	はい	はい
AWS::CodeBuild::ReportGroup	はい	はい
AWS::Cognito::IdentityPool	はい	いいえ
AWS::Cognito::UserPoolGroup	はい	いいえ
AWS::Config::ConfigurationRecorder	はい	はい
AWS::Config::ConformancePackCompliance	はい	はい
AWS::Config::ResourceCompliance	はい	はい
AWS::Connect::Instance	はい	いいえ
AWS::Connect::QuickConnect	はい	いいえ
AWS::Connect::User	はい	いいえ

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::DMS::Certificate	はい	はい
AWS::DMS::Endpoint	はい	はい
AWS::DMS::EventSubscription	はい	はい
AWS::DMS::ReplicationInstance	はい	はい
AWS::DMS::ReplicationSubnetGroup	はい	はい
AWS::DMS::ReplicationTask	はい	はい
AWS::DataSync::LocationEFS	はい	はい
AWS::DataSync::LocationFSxLustre	はい	はい
AWS::DataSync::LocationFSxWindows	はい	はい
AWS::DataSync::LocationHDFS	はい	はい
AWS::DataSync::LocationNFS	はい	はい
AWS::DataSync::LocationObjectStorage	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::DataSync::LocationS3	はい	はい
AWS::DataSync::LocationSMB	はい	はい
AWS::DataSync::Task	はい	はい
AWS::Detective::Graph	はい	はい
AWS::DynamoDB::Table	はい	はい
AWS::EC2::CapacityReservation	はい	はい
AWS::EC2::ClientVpnEndpoint	はい	はい
AWS::EC2::ClientVpnTargetNetworkAssociation	はい	はい
AWS::EC2::CustomerGateway	はい	はい
AWS::EC2::DHCPOptions	はい	はい
AWS::EC2::EC2Fleet	はい	はい
AWS::EC2::EIP	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::EC2::EgressOnlyInternetGateway	はい	はい
AWS::EC2::FlowLog	はい	はい
AWS::EC2::Host	はい	はい
AWS::EC2::IPAM	はい	はい
AWS::EC2::IPAMPool	はい	はい
AWS::EC2::IPAMResourceDiscovery	はい	はい
AWS::EC2::IPAMResourceDiscoveryAssociation	はい	はい
AWS::EC2::IPAMScope	はい	はい
AWS::EC2::Instance	はい	はい
AWS::EC2::InstanceConnectEndpoint	はい	はい
AWS::EC2::InternetGateway	はい	はい
AWS::EC2::LaunchTemplate	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::EC2::NatGateway	はい	はい
AWS::EC2::NetworkAcl	はい	はい
AWS::EC2::NetworkInterface	はい	はい
AWS::EC2::PrefixList	はい	はい
AWS::EC2::RouteTable	はい	はい
AWS::EC2::SecurityGroup	はい	はい
AWS::EC2::SnapshotBlockPublicAccess	はい	はい
AWS::EC2::SpotFleet	はい	はい
AWS::EC2::Subnet	はい	はい
AWS::EC2::SubnetRouteTableAssociation	はい	はい
AWS::EC2::TrafficMirrorFilter	はい	はい
AWS::EC2::TrafficMirrorSession	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::EC2::TrafficMirrorTarget	はい	はい
AWS::EC2::TransitGateway	はい	いいえ
AWS::EC2::TransitGatewayAttachment	はい	はい
AWS::EC2::TransitGatewayConnect	はい	はい
AWS::EC2::TransitGatewayMulticastDomain	はい	はい
AWS::EC2::TransitGatewayRouteTable	はい	はい
AWS::EC2::VPC	はい	はい
AWS::EC2::VPCBlockPublicAccessExclusion	はい	はい
AWS::EC2::VPCBlockPublicAccessOptions	はい	はい
AWS::EC2::VPCEndpoint	はい	はい
AWS::EC2::VPCEndpointConnectionNotification	はい	はい
AWS::EC2::VPCEndpointService	はい	いいえ

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::EC2::VPCPeeringConnection	はい	はい
AWS::EC2::VPNConnection	はい	はい
AWS::EC2::VPNConnectionRoute	はい	はい
AWS::EC2::VPNGateway	はい	はい
AWS::EC2::Volume	はい	はい
AWS::ECR::Repository	はい	はい
AWS::ECS::CapacityProvider	はい	はい
AWS::ECS::Cluster	はい	はい
AWS::ECS::Service	はい	はい
AWS::ECS::TaskDefinition	はい	はい
AWS::ECS::TaskSet	はい	はい
AWS::EFS::AccessPoint	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::EFS::FileSystem	はい	はい
AWS::EKS::Addon	はい	はい
AWS::EKS::Cluster	はい	はい
AWS::EKS::IdentityProviderConfig	はい	はい
AWS::EMR::SecurityConfiguration	はい	はい
AWS::ElasticBeanstalk::Application	はい	はい
AWS::ElasticBeanstalk::ApplicationVersion	はい	はい
AWS::ElasticBeanstalk::Environment	はい	はい
AWS::ElasticLoadBalancing::LoadBalancer	はい	はい
AWS::ElasticLoadBalancingV2::Listener	はい	はい
AWS::ElasticLoadBalancingV2::LoadBalancer	はい	はい
AWS::Elasticsearch::Domain	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::Events::EventBus	はい	はい
AWS::Events::Rule	はい	はい
AWS::FIS::ExperimentTemplate	はい	はい
AWS::Glue::Classifier	はい	はい
AWS::Glue::Job	はい	はい
AWS::Glue::MLTransform	はい	いいえ
AWS::GreengrassV2::ComponentVersion	はい	はい
AWS::GuardDuty::Detector	はい	はい
AWS::GuardDuty::Filter	はい	はい
AWS::GuardDuty::IPSet	はい	はい
AWS::GuardDuty::ThreatIntelSet	はい	はい
AWS::IAM::Group	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::IAM::InstanceProfile	いいえ	はい
AWS::IAM::OIDCProvider	いいえ	はい
AWS::IAM::Policy	はい	はい
AWS::IAM::Role	はい	はい
AWS::IAM::SAMLProvider	いいえ	はい
AWS::IAM::ServerCertificate	いいえ	はい
AWS::IAM::User	はい	はい
AWS::ImageBuilder::ContainerRecipe	はい	はい
AWS::ImageBuilder::DistributionConfiguration	はい	はい
AWS::ImageBuilder::ImagePipeline	はい	はい
AWS::ImageBuilder::ImageRecipe	はい	はい
AWS::ImageBuilder::InfrastructureConfiguration	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::InspectorV2::Activation	はい	はい
AWS::IoT::AccountAuditConfiguration	はい	はい
AWS::IoT::Authorizer	はい	はい
AWS::IoT::CACertificate	はい	はい
AWS::IoT::CustomMetric	はい	はい
AWS::IoT::Dimension	はい	はい
AWS::IoT::FleetMetric	はい	はい
AWS::IoT::JobTemplate	はい	はい
AWS::IoT::MitigationAction	はい	はい
AWS::IoT::Policy	はい	はい
AWS::IoT::ProvisioningTemplate	はい	はい
AWS::IoT::RoleAlias	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::IoT::ScheduledAudit	はい	はい
AWS::IoT::SecurityProfile	はい	はい
AWS::IoTEvents::AlarmModel	はい	いいえ
AWS::IoTEvents::DetectorModel	はい	いいえ
AWS::IoTEvents::Input	はい	いいえ
AWS::IoTSiteWise::AssetModel	はい	いいえ
AWS::IoTSiteWise::Gateway	はい	いいえ
AWS::IoTSiteWise::Portal	はい	いいえ
AWS::IoTTwinMaker::ComponentType	はい	いいえ
AWS::IoTTwinMaker::Entity	はい	いいえ
AWS::IoTTwinMaker::Workspace	はい	いいえ
AWS::KMS::Alias	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::KMS::Key	はい	はい
AWS::Kinesis::Stream	はい	はい
AWS::Kinesis::StreamConsumer	はい	はい
AWS::KinesisAnalyticsV2::Application	はい	はい
AWS::KinesisFirehose::DeliveryStream	はい	はい
AWS::Lambda::Function	はい	はい
AWS::Logs::Destination	はい	はい
AWS::MSK::BatchScramSecret	はい	はい
AWS::MSK::Cluster	はい	はい
AWS::MSK::ClusterPolicy	はい	はい
AWS::MSK::Configuration	はい	はい
AWS::MSK::VpcConnection	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::NetworkFirewall::Firewall	はい	はい
AWS::NetworkFirewall::FirewallPolicy	はい	はい
AWS::NetworkFirewall::RuleGroup	はい	はい
AWS::NetworkFirewall::VpcEndpointAssociation	はい	はい
AWS::NetworkManager::CustomerGatewayAssociation	はい	いいえ
AWS::NetworkManager::Device	はい	いいえ
AWS::NetworkManager::GlobalNetwork	はい	いいえ
AWS::NetworkManager::Link	はい	いいえ
AWS::NetworkManager::LinkAssociation	はい	いいえ
AWS::NetworkManager::Site	はい	いいえ
AWS::NetworkManager::TransitGatewayRegistration	はい	いいえ
AWS::OpenSearch::Domain	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::Pinpoint::App	はい	いいえ
AWS::Pinpoint::ApplicationSettings	はい	いいえ
AWS::Pinpoint::Campaign	はい	いいえ
AWS::Pinpoint::EmailChannel	はい	いいえ
AWS::Pinpoint::EmailTemplate	はい	いいえ
AWS::Pinpoint::EventStream	はい	いいえ
AWS::Pinpoint::InAppTemplate	はい	いいえ
AWS::Pinpoint::Segment	はい	いいえ
AWS::QuickSight::Template	はい	いいえ
AWS::RDS::DBCluster	はい	はい
AWS::RDS::DBClusterSnapshot	はい	はい
AWS::RDS::DBInstance	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::RDS::DBSecurityGroup	はい	はい
AWS::RDS::DBSnapshot	はい	はい
AWS::RDS::DBSubnetGroup	はい	はい
AWS::RDS::EventSubscription	はい	はい
AWS::RDS::OptionGroup	はい	はい
AWS::Redshift::Cluster	はい	はい
AWS::Redshift::ClusterParameterGroup	はい	はい
AWS::Redshift::ClusterSecurityGroup	はい	はい
AWS::Redshift::ClusterSnapshot	はい	はい
AWS::Redshift::ClusterSubnetGroup	はい	はい
AWS::Redshift::EventSubscription	はい	はい
AWS::Redshift::ScheduledAction	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::RoboMaker::RobotApplication	はい	いいえ
AWS::RoboMaker::RobotApplicationVersion	はい	いいえ
AWS::RoboMaker::SimulationApplication	はい	いいえ
AWS::Route53Profiles::Profile	はい	はい
AWS::Route53Resolver::FirewallDomainList	はい	はい
AWS::Route53Resolver::FirewallRuleGroup	はい	はい
AWS::Route53Resolver::FirewallRuleGroupAssociation	はい	はい
AWS::Route53Resolver::ResolverEndpoint	はい	はい
AWS::Route53Resolver::ResolverQueryLoggingConfig	はい	はい
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	はい	はい
AWS::Route53Resolver::ResolverRule	はい	はい
AWS::Route53Resolver::ResolverRuleAssociation	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::S3::AccessPoint	はい	はい
AWS::S3::AccountPublicAccessBlock	はい	はい
AWS::S3::Bucket	はい	はい
AWS::SES::ConfigurationSet	はい	いいえ
AWS::SES::ContactList	はい	いいえ
AWS::SES::Template	はい	いいえ
AWS::SNS::Topic	はい	はい
AWS::SQS::Queue	はい	はい
AWS::SSM::AssociationCompliance	はい	はい
AWS::SSM::Document	はい	はい
AWS::SSM::FileData	はい	はい
AWS::SSM::ManagedInstanceInventory	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::SSM::PatchCompliance	はい	はい
AWS::SageMaker::Model	はい	いいえ
AWS::SageMaker::NotebookInstance	はい	いいえ
AWS::SageMaker::NotebookInstanceLifecycleConfig	はい	いいえ
AWS::SecretsManager::Secret	はい	はい
AWS::SecurityHub::Standard	はい	はい
AWS::ServiceCatalog::CloudFormationProduct	はい	はい
AWS::ServiceCatalog::CloudFormationProvisionedProduct	はい	はい
AWS::ServiceCatalog::Portfolio	はい	はい
AWS::ServiceDiscovery::HttpNamespace	はい	はい
AWS::ServiceDiscovery::Instance	はい	はい
AWS::ServiceDiscovery::Service	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::StepFunctions::StateMachine	はい	はい
AWS::Transfer::Agreement	はい	はい
AWS::Transfer::Certificate	はい	はい
AWS::Transfer::Connector	はい	はい
AWS::Transfer::Profile	はい	はい
AWS::Transfer::Workflow	はい	はい
AWS::WAFRegional::RateBasedRule	はい	はい
AWS::WAFRegional::Rule	はい	はい
AWS::WAFRegional::RuleGroup	はい	はい
AWS::WAFRegional::WebACL	はい	はい
AWS::WAFv2::IPSet	はい	はい
AWS::WAFv2::ManagedRuleSet	はい	はい

リソースタイプ	AWS GovCloud (米国西部)	AWS GovCloud (米国東部)
AWS::WAFv2::RegexPatternSet	はい	はい
AWS::WAFv2::RuleGroup	はい	はい
AWS::WAFv2::WebACL	はい	はい
AWS::WorkSpaces::Workspace	はい	いいえ

を使用した AWS リソースの記録 AWS Config

AWS Config は、サポートされているリソースタイプの作成、変更、または削除を継続的に検出します。 は、これらのイベントを設定項目 (CI) として AWS Config 記録します。 CIs

は、サポートされているすべてのリソースタイプ、または関連するサポートされているリソースタイプのみの設定変更を記録する AWS Config ようにカスタマイズできます。が記録 AWS Config できるサポートされているリソースタイプのリストについては、「」を参照してください[でサポートされているリソースタイプ AWS Config](#)。

トピック

- 考慮事項
- リージョナルリソースとグローバルリソースの違い
- AWS Config ルールとグローバルリソースタイプ
- の記録頻度 AWS Config
- 記録されていないリソース
- AWS Config コンソールでのリソースの記録
- CLI AWS を使用したリソースの記録
- を使用した記録からのリソースの除外 AWS Config
- カスタマーマネージド設定レコーダーによる AWS Config 記録の停止

考慮事項

AWS Config 評価数が多い

AWS Config での最初の月の記録中に、後続の月と比較して、アカウントのアクティビティが増加することがあります。最初のブートストラッププロセス中に、 は、 が記録 AWS Config するように選択したアカウント内のすべてのリソースで評価 AWS Config を実行します。

エフェメラルワークロードを実行している場合、これらの一時リソースの作成と削除に関連する設定変更を記録する AWS Config ため、 からのアクティビティが増加することがあります。一時的なワークロードとは、必要なときにロードされて実行されるコンピューティングリソースを一時的に使用することです。例には、Amazon Elastic Compute Cloud (Amazon EC2) スポットインスタンス、Amazon EMR ジョブ、 AWS Auto Scalingがあります。

一時的なワークロードの実行によるアクティビティの増加を回避するには、カスタマーマネージド設定レコーダーを設定してこれらのリソースタイプが記録されないようにするか、これらのタイプのワークロードをオフ AWS Config の別のアカウントで実行して、設定記録とルール評価の増加を回避できます。

利用可能なリージョン

が追跡 AWS Config するリソースタイプを指定する前に、リージョン別のリソースカバレッジの可用性をチェックして、リソースタイプがセットアップした AWS リージョンでサポートされているかどうかを確認します AWS Config。

リソースタイプが少なくとも 1 つのリージョン AWS Config で でサポートされている場合は、指定したリソースタイプがセットアップしたリージョンでサポートされていない場合でも AWS Config、でサポートされているすべての AWS リージョンでそのリソースタイプの記録を有効にできます AWS Config。

リージョナルリソースとグローバルリソースの違い

リージョナルリソース

リージョナルリソースは特定のリージョンに結び付けられており、そのリージョンでのみ使用できます。指定した に作成し AWS リージョン、そのリージョンに存在します。これらのリソースの表示や操作を行うには、そのリージョンに対してオペレーションを指示する必要があります。たとえば、 を使用して Amazon EC2 インスタンスを作成するには AWS Management Console、インスタンスを作成する を選択します AWS リージョン。 AWS Command Line Interface（ AWS CLI) を使用してインスタンスを作成する場合は、 `--region`パラメータを含めます。 AWS

SDKs はそれぞれ、オペレーションが使用するリージョンを指定するための独自の同等のメカニズムを持っています。

リージョナルリソースを使用するのは、いくつかの理由があります。理由の 1 つは、リソースと、そのリソースへのアクセスに使用するサービスエンドポイントを、できるだけ顧客の近くに置くことです。これにより、レイテンシーが最小限に抑えられるため、パフォーマンスが向上します。もう 1 つの理由は、分離境界を設けることです。これにより、複数のリージョンに独立したリソースのコピーを作成することで、負荷を分散してスケーラビリティを向上させることができます。同時に、リソースを互いに分離することで可用性を向上させます。

AWS リージョン コンソールまたは AWS CLI コマンドで別の を指定した場合、前のリージョンに表示されるリソースを表示したり操作したりできなくなります。

リージョナルリソースの Amazon リソースネーム (ARN) を表示すると、そのリソースを含むリージョンが ARN の 4 番目のフィールドとして指定されています。例えば、Amazon EC2 インスタンスはリージョナルリソースです。以下に示しているのは、`us-east-1` リージョンに存在する Amazon EC2 インスタンス用の ARN の例です。

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

グローバルリソース

一部の AWS サービスリソースはグローバルリソースです。つまり、どこからでもリソースを使用できます。グローバルサービスのコンソールでは AWS リージョン を指定しません。グローバルリソースにアクセスするには、サービスの AWS CLI および AWS SDK オペレーションを使用するときに`--region`パラメータを指定しません。

グローバルリソースは、特定のリソースのインスタンスが一度に 1 つしか存在できないことが必須なケースをサポートします。このようなシナリオでは、異なるリージョンのコピーとの間でレプリケーションや同期を行うことは適切ではありません。リソースのコンシューマーが変更内容を瞬時に確認できるようにするとレイテンシーが増加する可能性があるため、単一のグローバルエンドポイントにアクセスする必要があることは許容できると考えられます。

例えば、Amazon Aurora グローバルクラスター (`AWS::RDS::GlobalCluster`) はグローバルリソースのため、リージョンには関連付けられません。これは、リージョンのエンドポイントに依存することなく、グローバルクラスターを作成できるということになります。Amazon Relational Database Service (Amazon RDS) 自体はリージョンごとに構成されている一方で、グローバルクラスターを生成した特定のリージョンによってグローバルクラスターに影響を与えないという利点があります。これは、すべてのリージョンにまたがる 1 つの連続したグローバルクラスターのように見えます。

グローバルリソースの Amazon リソースネーム (ARN) には、リージョンは含まれません。以下のグローバルクラスターの ARN の例のように、4 番目のフィールドは空です。

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> 2022 年 2 月 AWS Config 以降に にオンボードされたグローバルリソースタイプは、商用パーティションの場合はサービスのホームリージョンに、 GovCloud パーティションの場合は AWS GovCloud (米国西部) にのみ記録されます。これらの新しいグローバルリソースタイプの設定項目 (CIs) は、ホームリージョンと AWS GovCloud (米国西部) でのみ表示できます。
> 2022 年 2 月より前にオンボードされたグローバルリソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および `AWS::IAM::User`) は変更されません。2022 年 2 月より前に AWS Config がサポートされているすべてのリージョンで、これらのグローバル IAM リソースの記録を有効にできます。これらのグローバル IAM リソースは、2022 年 2 月 AWS Config 以降、 でサポートされているリージョンでは記録できません。

グローバルリソースタイプ | IAM リソース

IAM ユーザー、グループ、ロール、およびカスタマー管理ポリシーの IAM リソースタイプはグローバルリソースです。これらのリソースタイプは、 が 2022 年 2 月より前に利用可能 AWS Config であったリージョンで、 によって AWS Config 記録できます。グローバル IAM リソースタイプを記録できないこのリストには、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、アジアパシフィック (タイ) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) 、イスラエル (テルアビブ) 、メキシコ (中部) 、中東 (アラブ首長国連邦) の各リージョンが含まれます。

設定項目 (CI) の重複を防ぐために、サポートされる 1 つのリージョンで一度にグローバル IAM リソースを記録することだけを考慮する必要があります。また、不必要な評価や API スロットリングを回避するのにも役立ちます。

グローバルリソースタイプ | ホームリージョンのみ

次のサービスのグローバルリソースは、Amazon Elastic Container Registry Public、Amazon Route 53 AWS Global Accelerator、Amazon CloudFront、および のグローバルリソースタ

イプのホームリージョンでのみ AWS Config によって記録されます AWS WAF。これらのグローバルリソースでは、リソースタイプの同じインスタンスを複数の AWS リージョンで使用できますが、設定項目 (CIs) は商用パーティションのホームリージョンまたは AWS GovCloud (US) パーティションの AWS GovCloud (米国西部) にのみ記録されます。

グローバルリソースタイプのホームリージョン

AWS サービス	リソースタイプの値	ホームリージョン
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	米国東部 (バージニア北部) リージョン
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	米国西部 (オレゴン) リージョン
	`AWS::GlobalAccelerator::EndpointGroup`	米国西部 (オレゴン) リージョン
	`AWS::GlobalAccelerator::Accelerator`	米国西部 (オレゴン) リージョン
Amazon Route 53	`AWS::Route53::HostedZone`	米国東部 (バージニア北部) リージョン
	`AWS::Route53::HealthCheck`	米国東部 (バージニア北部) リージョン
Amazon CloudFront	`AWS::CloudFront::Distribution`	米国東部 (バージニア北部) リージョン
AWS WAF	`AWS::WAFv2::WebACL`	米国東部 (バージニア北部) リージョン

グローバルリソースタイプ | Aurora グローバルクラスター

`AWS::RDS::GlobalCluster` は、カスタマーマネージド設定レコーダーが有効になっているサポートされているすべての AWS Config リージョンに記録されるグローバルリソースです。このグローバルリソースタイプは、1 つのリージョンでこのリソースの記録を有効にする

と、 AWS Config は有効なすべてのリージョンでこのリソースタイプの設定項目 (CIs) を記録するという点で一意です。

有効なすべてのリージョンで `AWS::RDS::GlobalCluster` を記録しない場合は、次のいずれかの AWS Config コンソールの記録方法を使用します。

- カスタマイズ可能なオーバーライドを使用してすべてのリソースタイプを記録し、AWS「RDS GlobalCluster」を選択し、オーバーライド「記録から除外」を選択します。
- [特定のリソースタイプを記録する]。

有効なすべてのリージョンで `AWS::RDS::GlobalCluster` を記録しない場合、API/CLI に対して次のいずれかの記録方法を使用します。

- 除外を伴う、現在および将来のリソースタイプを記録する (`EXCLUSION_BY_RESOURCE_TYPES`)
- [特定のリソースタイプを記録する] (`INCLUSION_BY_RESOURCE_TYPES`)。

AWS Config ルールとグローバルリソースタイプ

2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および `AWS::IAM::User`) は、2022 年 2 月より前に AWS Config が利用可能なリージョンでのみ AWS Config によって記録できます。これらのグローバル IAM リソースタイプは、2022 年 2 月 AWS Config 以降、 でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、「Recording AWS Resources | Global Resources」を参照してください。

少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。

2022 年 2 月より前のグローバルリソースオンボードに関するコンプライアンスを報告するためのベストプラクティス

不要な評価を回避するには、これらのグローバルリソースが対象範囲内にある AWS Config ルールとコンフォーマンスパックのみを、サポートされているリージョンの 1 つにデプロイする必要があります。どのマネージドルールがどのリージョンでサポートされているかのリストについては、「List of AWS Config Managed Rules by Region Availability」を参照してください。これは、 AWS Config ルール、組織 AWS Config ルール、および AWS Security Hub や などの他の AWS サービスによって作成されたルールにも適用されます AWS Control Tower。

2022 年 2 月より前にオンボーディングされたグローバルリソースタイプを記録しない場合は、不要な評価を回避するために、次の定期ルールを有効にしないことをお勧めします。

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

2022 年 2 月より後のグローバルリソースオンボードに関するコンプライアンスを報告するためのベストプラクティス

2022 年 2 月以降に AWS Config 録画にオンボードされたグローバルリソースタイプは、商用パーティションの場合はサービスのホームリージョンに、 AWS GovCloud (US) パーティションの場合は AWS GovCloud (米国西部) にのみ記録されます。これらのグローバルリソースがスコープ内にある AWS Config ルールとコンフォーマンスパックは、リソースタイプのホームリージョンにのみデプロイする必要があります。詳細については、「Home Regions for Global Resource Types」を参照してください。

の記録頻度 AWS Config

AWS Config は、連続録画と日次録画をサポートしています。継続的な記録により、変更が発生するたびに設定の変更を継続的に記録できます。日時記録により、以前に記録された CI と異なる場合にのみ、過去 24 時間におけるリソースの最新の状態を表す設定項目 (CI) を、受け取ることができます。録画頻度を変更する手順については、「Changing Recording Frequency」を参照してください。

継続的な記録

継続的な記録のメリットには次が含まれます。

- リアルタイムモニタリング: 継続的な記録は、不正な変更や予期しない変更を即時に検出できるため、セキュリティとコンプライアンスへの取り組みを強化できます。
- 詳細な分析: 継続的な記録は、リソースへの設定変更が発生したときに詳細に分析できるため、その時点でのパターンや傾向を識別できます。

日次記録

日次記録のメリットには次が含まれます。

- 最小限の中断: 日次記録により、情報の流れを管理しやすくなるため、通知の頻度とアラートの疲労を軽減できます。
- コスト効率: 日次記録は、リソースへの変更をより低い頻度で柔軟に記録できるため、記録される設定変更の数に関連するコストを削減できます。

> **Note**
>
> AWS Firewall Manager は、リソースをモニタリングするために継続的な記録に依存します。Firewall Manager を使用している場合、記録頻度を連続に設定することをお勧めします。

記録されていないリソース

リソースが記録されていない場合、 はそのリソースの作成と削除のみを AWS Config キャプチャし、その他の詳細はキャプチャしません。記録されていないリソースが作成または削除されると、は通知 AWS Config を送信し、リソースの詳細ページにイベントを表示します。記録対象外のリソースの詳細ページでは、ほとんどの設定詳細について null 値が表示され、関係や設定変更に関する情報は表示されません。

が記録済みリソース AWS Config に提供する関係情報は、記録されていないリソースのデータがないため、制限されません。記録対象のリソースが記録対象外のリソースに関連付けられている場合、その関係は記録対象のリソースの詳細ページに表示されます。

IAM リソースタイプの考慮事項

`AWS::IAM::User`、`AWS::IAM::Policy`、 `AWS::IAM::Group`、 `AWS::IAM::Role`リソースタイプは、リソースがカスタマーマネージド設定レコーダー に記録するリソースとして選

択されているか、以前に選択されていた場合にのみ、作成 (`ResourceNotRecorded`) と削除 (`ResourceDeletedNotRecorded`) の状態をキャプチャします。

記録されていないリソースの CI 記録スケジュール

`ResourceNotRecorded` および `ResourceDeletedNotRecorded` の設定項目 (CI) は、リソースタイプの一般的な記録時間に従っていません。これらのリソースタイプは、カスタマーマネージド設定レコーダーの定期的なベースラインプロセス中にのみ記録されます。これは、他のリソースタイプよりも頻度が低くなります。つまり、作成または削除通知は、作成または削除時ではなく、ベースライン作成プロセス中に送信されます。

CI 配信とサービスにリンクされたレコーダーの範囲

サービスにリンクされた設定レコーダーの場合、記録スコープは、配信チャネルで設定項目 (CIs) を受信するかどうかを決定します。記録スコープは、設定レコーダーにリンクされているサービスによって設定されます。記録スコープが内部の場合、配信チャネルで CIsを受信しません。

AWS Config コンソールでのリソースの記録

AWS Config コンソールを使用して、カスタマーマネージド設定レコーダー AWS Config に記録するリソースのタイプを選択できます。

リソースを選択するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. 左側のナビゲーションペインの [設定] を選択します。
3. カスタマーマネージドレコーダータブで、編集 を選択します。
4. [記録方法] セクションで、記録方法を選択します。 AWS Config 記録する AWS リソースを指定できます。

   All resource types with customizable overrides

   このリージョンで現在および将来サポートされているすべてのリソースタイプの設定変更を記録する AWS Config ように を設定します。特定のリソースタイプの記録頻度をオーバーライドしたり、特定のリソースタイプを記録から除外したりできます。詳細については、[サポートされるリソースタイプ] を参照してください。

   - デフォルト設定

現在および将来サポートされるすべてのリソースタイプについて、デフォルトの記録頻度を設定します。詳細については、「Recording Frequency」を参照してください。

- 継続的な記録 — 変更が発生するたびに、設定の変更を継続的に記録 AWS Config します。
- 日時記録 - 以前に記録された CI と異なる場合にのみ、過去 24 時間におけるリソースの最新の状態を表す設定項目 (CI) を、受け取ります。

> **Note**
>
> AWS Firewall Manager は、リソースをモニタリングするために継続的な記録に依存します。Firewall Manager を使用している場合、記録頻度を連続に設定することをお勧めします。

- 上書き設定

  特定のリソースタイプの記録頻度を上書きしたり、特定のリソースタイプを記録から除外したりします。リソースタイプの記録頻度を変更するか、またはリソースタイプの記録を停止した場合、既に記録されている設定項目は変更されません。

Specific resource types

指定したリソースタイプのみの設定変更を記録する AWS Config ように を設定します。

- 特定のリソースタイプ

  記録するリソースタイプとその頻度を選択します。詳細については、「Recording Frequency」を参照してください。

  - 継続的な記録 — 変更が発生するたびに、設定の変更を継続的に記録 AWS Config します。
  - 日時記録 - 以前に記録された CI と異なる場合にのみ、過去 24 時間におけるリソースの最新の状態を表す設定項目 (CI) を、受け取ります。

> **Note**
>
> AWS Firewall Manager は、リソースをモニタリングするために継続的な記録に依存します。Firewall Manager を使用している場合、記録頻度を連続に設定することをお勧めします。

リソースタイプの記録頻度を変更するか、またはリソースタイプの記録を停止した場合、既に記録されている設定項目は変更されません。

5. [保存] を選択して変更を保存します。

リソースを記録する際の考慮事項

AWS Config 評価の数が多い

AWS Config での最初の月の記録中に、後続の月と比較して、アカウントのアクティビティが増加することがあります。最初のブートストラッププロセス中に、 は、 が記録 AWS Config するために選択したアカウント内のすべてのリソースで評価 AWS Config を実行します。

エフェメラルワークロードを実行している場合、これらの一時リソースの作成と削除に関連する設定変更を記録する AWS Config ため、 からのアクティビティが増加することがあります。一時的なワークロードとは、必要なときにロードされて実行されるコンピューティングリソースを一時的に使用することです。例としては、Amazon Elastic Compute Cloud (Amazon EC2) スポットインスタンス、Amazon EMR ジョブ、 AWS Auto Scalingなどがあります。一時的なワークロードの実行によるアクティビティの増加を回避するには、カスタマーマネージド設定レコーダーを設定してこれらのリソースタイプが記録されないようにするか、これらのタイプのワークロードを AWS Config オフの別のアカウントで実行して、設定の記録とルール評価の増加を回避できます。

Considerations: All resource types with customizable overrides

グローバルに記録するリソースタイプ | Aurora グローバルクラスターは、最初は記録に含められます

`AWS::RDS::GlobalCluster` リソースタイプは、カスタマーマネージド設定レコーダーが有効になっているサポートされているすべての AWS Config リージョンに記録されます。

すべての有効なリージョンで `AWS::RDS::GlobalCluster` を記録しない場合、「AWS RDS GlobalCluster」を選択し、「記録から除外する」というオーバーライドを選択します。

グローバルリソースタイプ | IAM リソースタイプは、最初は記録から除外されます。

コスト削減のため、グローバル IAM リソースタイプは、最初は記録から除外されます。このバンドルには、IAM ユーザー、グループ、ロール、およびカスタマー管理ポリシーが含まれます。[削除] を選択してオーバーライドを削除し、これらのリソースを記録に含めます。

さらに、グローバル IAM リソースタイプ (`AWS::IAM::User`、`AWS::IAM::Group`、`AWS::IAM::Role`、および `AWS::IAM::Policy`) は、2022 年 2 月 AWS Config 以降に でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。

制限

最大 100 の頻度のオーバーライドと 600 の除外のオーバーライドを追加できます。

次のリソースタイプに日次記録はサポートされていません。

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

利用可能なリージョン

が追跡 AWS Config するリソースタイプを指定する前に、Resource Coverage by Region Availability をチェックして、リソースタイプがセットアップした AWS リージョンでサポートされているかどうかを確認します AWS Config。リソースタイプが少なくとも 1 つのリージョン AWS Config で でサポートされている場合は、指定したリソースタイプがセットアップしたリージョンでサポートされていない場合でも AWS Config、 でサポートされているすべての AWS リージョンでそのリソースタイプの記録を有効にできます AWS Config。

制限

すべてのリソースタイプが同じ頻度であれば制限はありません。少なくとも 1 つのリソースタイプが継続に設定されている場合、日次の頻度で最大 100 のリソースタイプを追加できます。

次のリソースタイプに日次頻度はサポートされていません。

- AWS::Config::ResourceCompliance
- AWS::Config::ConformancePackCompliance
- AWS::Config::ConfigurationRecorder

CLI AWS を使用したリソースの記録

AWS CLI を使用して、 AWS Config 記録するリソースのタイプを選択できます。これを行うには、カスタマーマネージド設定レコーダーを作成します。このレコーダーは、記録グループで指定したリソースのタイプを記録します。記録グループ内では、サポートされているすべてのリソースタイプを記録するのか、特定のリソースタイプのみを含めるか、または除外するかを指定します。

Record all current and future supported resource types

このリージョンで現在および今後サポートされているすべてのリソースタイプの設定変更を記録する AWS Config ように を設定します。サポートされているリソースタイプのリストについては、「サポートされているリソースタイプ」を参照してください。

1. put-configuration-recorderコマンドを使用します。

   このコマンドは、[--configuration-recorder] フィールドと [---recording-group] フィールドを使用します。

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   configuration-recorderフィールド

   [configurationRecorder.json] ファイルは、name および roleArn、さらに設定レコーダーのデフォルトの記録頻度を指定します (recordingMode)。

   ```
   {
     "name": "default",
     "roleARN": "arn:aws:iam::123456789012:role/config-role",
     "recordingMode": {
       "recordingFrequency": CONTINUOUS or DAILY,
       "recordingModeOverrides": [
           {
               "description": "Description you provide for the override",
   ```

```
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

recording-groupフィールド

recordingGroup.json ファイルは、記録されるリソースタイプを指定します。

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

これらのフィールドの詳細については、AWS CLI 「 コマンドリファレンスput-configuration-recorder」の「」を参照してください。

2. (オプション) カスタマーマネージド設定レコーダーに必要な設定があることを確認するには、次のdescribe-configuration-recordersコマンドを使用します。

```
$ aws configservice describe-configuration-recorders
```

以下に、応答の例を示します。

```
{
    "ConfigurationRecorders": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
```

```
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

記録から除外 AWS Config するように指定するリソースタイプを除く、グローバルリソースタイプを含む、現在および将来サポートされているすべてのリソースタイプの設定変更を記録するように を設定します。

リソースタイプの記録を停止することを選択した場合、既に記録されている設定項目は変更されません。サポートされているリソースタイプのリストについては、「サポートされているリソースタイプ」を参照してください。

1. put-configuration-recorderコマンドを使用します。

   このコマンドは、[--configuration-recorder] フィールドと [---recording-group] フィールドを使用します。

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   configuration-recorderフィールド

[configurationRecorder.json] ファイルは、name および roleArn、さらに設定レコーダーのデフォルトの記録頻度を指定します (recordingMode)。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

recording-groupフィールド

recordingGroup.json ファイルは、記録 AWS Config するリソースのタイプを指定します。次の例に示すようにexclusionByResourceTypes、 の resourceTypesフィールドで除外する 1 つ以上のリソースタイプを渡します。

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

これらのフィールドの詳細については、AWS CLI 「 コマンドリファレンスput-configuration-recorder」の「」を参照してください。

2. (オプション) カスタマーマネージド設定レコーダーに必要な設定があることを確認するには、次のdescribe-configuration-recordersコマンドを使用します。

```
$ aws configservice describe-configuration-recorders
```

以下に、応答の例を示します。

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
```

```
    ]
}
```

Record specific resource types

指定したリソースタイプのみの設定変更を記録する AWS Config ように を設定します。

リソースタイプの記録を停止することを選択した場合、既に記録されている設定項目は変更されません。サポートされているリソースタイプのリストについては、「サポートされているリソースタイプ」を参照してください。

1. put-configuration-recorderコマンドを使用します。

   このコマンドは、[--configuration-recorder] フィールドと [---recording-group] フィールドを使用します。

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   configuration-recorderフィールド

   [configurationRecorder.json] ファイルは、name および roleArn、さらに設定レコーダーのデフォルトの記録頻度を指定します (recordingMode)。

   ```
   {
     "name": "default",
     "roleARN": "arn:aws:iam::123456789012:role/config-role",
     "recordingMode": {
       "recordingFrequency": CONTINUOUS or DAILY,
       "recordingModeOverrides": [
           {
               "description": "Description you provide for the override",
               "recordingFrequency": CONTINUOUS or DAILY,
               "resourceTypes": [ Comma-separated list of resource types to include
    in the override ]
           }
       ]
     }
   }
   ```

recording-groupフィールド

recordingGroup.json ファイルは、記録 AWS Config するリソースのタイプを指定します。次の例に示すように、 resourceTypesフィールドで除外する 1 つ以上のリソースタイプを渡します。

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

これらのフィールドの詳細については、AWS CLI 「 コマンドリファレンスput-configuration-recorder」の「」を参照してください。

2. (オプション) カスタマーマネージド設定レコーダーに必要な設定があることを確認するには、次のdescribe-configuration-recordersコマンドを使用します。

```
$ aws configservice describe-configuration-recorders
```

以下に、応答の例を示します。

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
```

```
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

を使用した記録からのリソースの除外 AWS Config

AWS Config では、インベントリ追跡とコンプライアンスモニタリングから特定のタイプの AWS リソースを除外しながら、将来追加されるリソースを含め AWS Config、現在利用可能な他のすべてのサポートされているリソースタイプを追跡できます。この機能を使用すると、コンプライアンスおよびガバナンスの基準が適用される重要なリソースに注力できます。

Excluding resources (Console)

AWS リソースタイプを記録しない場合は、 AWS Config コンソールで次のいずれかの記録戦略を使用します。

- カスタマイズ可能なオーバーライドを使用してすべてのリソースタイプを記録し、除外するリソースタイプを選択し、オーバーライド「記録から除外」を選択します
- [特定のリソースタイプを記録する]。

詳細については、「リソースの記録 (コンソール)」を参照してください。

Excluding resources (AWS CLI)

AWS リソースタイプを記録しない場合は、API/CLI に次のいずれかの記録戦略を使用します。

- 除外を伴う、現在および将来のリソースタイプを記録する (`EXCLUSION_BY_RESOURCE_TYPES`)
- [特定のリソースタイプを記録する] (`INCLUSION_BY_RESOURCE_TYPES`)。

詳細については、「リソースの記録 (AWS CLI)」を参照してください。

カスタマーマネージド設定レコーダーによる AWS Config 記録の停止

カスタマーマネージド設定レコーダーへの AWS Config 記録はいつでも停止できます。がリソースの記録 AWS Config を停止すると、以前にキャプチャされた設定情報が保持され、この情報に引き続きアクセスできます。

記録を停止する手順については、「カスタマーマネージド設定レコーダーの停止」を参照してください。

を使用したサードパーティーリソース AWS Config の による設定の記録 AWS CLI

サードパーティーのリソース、またはオンプレミスサーバー、SAAS モニタリングツール、バージョン管理システム (GitHub など) などのカスタムリソースタイプの設定を記録します。

AWS Config コンソール AWS Config と APIs を使用して、サードパーティーリソースの設定データを に公開し、リソースインベントリと設定履歴を表示およびモニタリングできます。 AWS Config

を使用してすべてのリソースを管理し、 AWS Config ルールを使用してベストプラクティスへの準拠についてリソース設定を評価できます。 AWS Config ルールまたはコンフォーマンスパックを作成して、これらのサードパーティーリソースをベストプラクティス、内部ポリシー、規制ポリシーに照らして評価することもできます。

> **Note**
>
> すべてのリソースタイプを記録する AWS Config ように を設定している場合、 を通じて管理 (作成、更新、または削除) されるサードパーティーリソース AWS CloudFormation は、で設定項目 AWS Config として自動的に追跡されます。

前提条件： サードパーティーリソースまたはカスタムリソースタイプは、 を使用して登録する必要があります AWS CloudFormation。

トピック

- へのサードパーティーリソースの追加 AWS Config
- を使用してサードパーティーリソース AWS Config の設定項目を で記録する AWS CLI
- を使用してサードパーティーリソース AWS Config の設定項目を読み取る AWS CLI
- を使用して から AWS Config サードパーティーリソースを削除する AWS CLI

へのサードパーティーリソースの追加 AWS Config

AWS Configにサードパーティーリソースを追加するには、次の手順に従います。

トピック

- ステップ 1: 開発環境をセットアップする
- ステップ 2: リソースをモデル化する
- ステップ 3: アーティファクトを生成する
- ステップ 4: リソースを登録する
- ステップ 5: リソース設定を公開する

ステップ 1: 開発環境をセットアップする

AWS CloudFormation AWS CLIをインストールして設定します。 AWS CLI を使用すると、カスタムリソースをモデル化して登録できます。詳細については、カスタムリソースおよび CloudFormation Command Line Interface とはを参照してください。

ステップ 2: リソースをモデル化する

リソースタイプの設定に準拠し検証するリソースプロバイダスキーマを作成します。

1. `init` コマンドを使用して、リソースプロバイダプロジェクトを作成し、必要なファイルを生成します。

```
$ cfn init
Initializing new project
```

2. `init` コマンドを実行すると、ウィザードが起動し、リソース名の指定など、プロジェクトの設定手順が示されます。このウォークスルーでは、`MyCustomNamespace::Testing::WordPress` を指定してください。

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. リソースのパッケージ名を入力します。

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> プロジェクトの依存関係を正しく解決できるようにするために、生成されたプロジェクトを Maven サポートを使用して IDE にインポートできます。
> 例えば、IntelliJ IDEA を使用している場合は、次の操作を行う必要があります。
>
> - [File] (ファイル) メニューから [New] (新規) を選択し、[Project From Existing Sources] (既存のソースからのプロジェクト) を選択します。
> - プロジェクトディレクトリへの移動

- [Import Project] (プロジェクトのインポート) ダイアログボックスで、[Import project from external model] (外部モデルからプロジェクトをインポート)、[Maven] の順に選択します。
- [Next] (次へ) を選択してデフォルトを承諾し、プロジェクトの読み込みを完了します。

4. リソースのスキーマを含む `mycustomnamespace-testing-wordpress.json` ファイルを開きます。次のスキーマをコピーして `mycustomnamespace-testing-wordpress.json` に貼り付けます。

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. スキーマを検証します。

```
$ cfn validate
```

6. リソースプロバイダパッケージ内の自動生成されたファイルを更新して、リソースプロバイダスキーマの更新を表示します。リソースプロバイダープロジェクトの開始時、 はリソースプロバイダーのサポートファイルとコード AWS CLI を生成します。コードを再生成して、更新されたスキーマを確認します。

```
$ cfn generate
```

> **Note**
>
> Maven を使用する場合、`generate` コマンドは構築プロセスの一部としてコードがコンパイルされる前に自動的に実行されます。そのため、変更内容は生成されたコードと同期しません。
> CloudFormation CLI は、Maven/システムが見つけることができる場所に配置する必要があります。詳細については、拡張機能を開発するための環境のセットアップを参照してください。

プロセス全体の詳細については、AWS CloudFormationで使用するためのモデリングリソースプロバイダーを参照してください。

ステップ 3: アーティファクトを生成する

次のコマンドを実行して `cfn submit` のアーティファクトを生成します。

```
$ mvn package
```

ステップ 4: リソースを登録する

AWS Config では、リソースプロバイダーハンドラーがリソースの設定追跡を実行する必要はありません。次のコマンドを実行して、リソースを登録します。

```
$ cfn submit
```

詳細については、AWS CloudFormation 「 テンプレートで使用するリソースプロバイダーの登録」を参照してください。

ステップ 5: リソース設定を公開する

MyCustomNamespace::Testing::WordPress の設定を特定します。

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

スキーマバージョン ID を決定します AWS CloudFormation `DescribeType`。

では AWS Config、このリソース設定が受け入れられているかどうかを確認できます。コンプライアンスを評価するには、このリソースを使用して AWS Config ルールを記述します。

(オプション) 設定の記録を自動化するには、定期的または変更ベースの設定コレクターを実装します。

を使用してサードパーティーリソース AWS Config の設定項目を で記録する AWS CLI

次の手順を使用して、サードパーティーリソースまたはカスタムリソースタイプの構成項目を記録します。

リソースタイプ `MyCustomNamespace::Testing::WordPress` を対応するスキーマに登録してください。

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. 次のコマンドを入力します。

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> タイプスキーマで定義されているように、 `writeOnlyProperties` は によって記録される前に設定から削除されます AWS Config。つまり、読み取り API から設定を取得する場合、これらの値は存在しません。`writeOnlyProperties` の詳細については、リソースタイプのスキーマを参照してください。

を使用してサードパーティーリソース AWS Config の設定項目を読み取る AWS CLI

次の手順を使用して、サードパーティーリソースまたはカスタムリソースタイプの構成項目を読み取ります。

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. 次のコマンドを入力します。

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. [Enter] キーを押します。

   次のような出力が表示されます:

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. 次のコマンドを入力します。

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. [Enter] キーを押します。

次のような出力が表示されます:

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

を使用して から AWS Config サードパーティーリソースを削除する AWS CLI

次のコマンドを入力して、サードパーティーリソースを削除します。

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

成功すると、コマンドは追加の出力なしで実行されます。

を使用したマネージドインスタンスのソフトウェア設定の記録 AWS Config

を使用して AWS Config 、Amazon EC2 インスタンスとオンプレミスサーバーでソフトウェアインベントリの変更を記録できます。これにより、ソフトウェア設定の変更履歴を確認できます。例えば、新しい Windows 更新プログラムがマネージド Windows インスタンスにインストールされる

と、 は変更 AWS Config を記録してから配信チャネルに送信し、変更について通知されるようにします。を使用すると AWS Config、マネージドインスタンスに Windows 更新プログラムがインストールされた日時と、時間の経過とともにどのように変更されたかの履歴を確認できます。

トピック

- 前提条件
- ソフトウェア設定の記録

前提条件

ソフトウェア設定の変更を記録するには、次のステップを完了する必要があります。

- AWS Configでマネージドインスタンスのインベントリリソースタイプの記録をオンにします。
- EC2 サーバーとオンプレミスサーバーを のマネージドインスタンスとして設定します AWS Systems Manager。マネージドインスタンスとは、Systems Manager で使用するために設定されたマシンです。
- Systems Manager インベントリ機能を使用して、マネージドインスタンスからソフトウェアインベントリの収集を開始します。

> **Note**
>
> Systems Manager が、アンマネージドインスタンスの設定項目の作成をサポートするようになりました
> アンマネージインスタンスの設定項目には、`Key: “InstanceStatus”` と `Value: “Unmanaged”` の補助的な設定が含まれます。
> アンマネージドインスタンスの設定項目は追加の更新を受け取りません
> 追加の更新を受け取るには、設定項目がマネージドインスタンスである必要があります。

AWS Config ルールを使用してソフトウェア設定の変更をモニタリングし、変更がルールに準拠しているかどうかを通知することもできます。例えば、マネージドインスタンスに指定のアプリケーションがあるかどうかを確認するルールを作成すると、インスタンスに指定のアプリケーションがインストールされていない場合に、 AWS Config はインスタンスがルールに準拠していないことをフラグで知らせます。 AWS Config マネージドルールのリストについては、「」を参照してくださいAWS Config マネージドルールのリスト。

ソフトウェア設定の記録

AWS Configでソフトウェアの設定変更の記録を有効にするには

1. AWS Configですべてのサポートされているリソースタイプの記録を有効にするか、一部の選択したマネージドインスタンスのインベントリリソースタイプを記録します。詳細については、「を使用した AWS リソースの記録 AWS Config」を参照してください。
2. Systems Manager のインスタンスプロファイルを使用して Amazon EC2 インスタンスを起動します。このプロファイルには、AmazonSSMManagedInstanceCore管理ポリシーが含まれています。この AWS 管理ポリシーにより、インスタンスは Systems Manager サービスコア機能を使用できます。

   Systems Manager のインスタンスプロファイルに追加できるその他のポリシーについては、AWS Systems Manager ユーザーガイドの [Create an IAM Instance Profile for System Manager (Systems Manager の IAM インスタンスプロファイルの作成)] を参照してください。

   > **Important**
   >
   > SSM Agent は、クラウド上の System Manager と通信するために、マネージドインスタンスにインストールする必要がある Amazon ソフトウェアです。次のいずれかのオペレーティングシステム用の AMI から EC2 インスタンスが作成された場合、このエージェントがプリインストールされています。
   >
   > - 2016 年 11 月以降に公開された Windows Server 2003-2012 R2 AMI
   > - Windows Server 2016 および 2019
   > - Amazon Linux
   > - Amazon Linux 2
   > - Ubuntu Server 16.04
   > - Ubuntu Server 18.04
   >
   > このエージェントがプリインストールされた AMI から作成されていない EC2 インスタンスでは、エージェントを手動でインストールする必要があります。詳細については、AWS Systems Manager ユーザーガイドの次の [トピック] を参照してください。
   >
   > - EC2 インスタンスでの SSM Agent のインストールと設定 (Windows Server 用)
   > - EC2 インスタンスでの SSM Agent のインストールと設定 (Linux 用)

3. AWS Systems Manager ユーザーガイドの [インベントリ収集の設定] に従ってインベントリ収集を開始します。手順は、Linux インスタンスでも Windows インスタンスでも同じです。

   AWS Config は、次のインベントリタイプの設定変更を記録できます。

   - [Applications (アプリケーション)] - マネージドインスタンスのアプリケーション (ウイルス対策ソフトウェアなど) のリスト。
   - AWS components – AWS CLI や SDKs など、マネージドインスタンスのコンポーネントのリスト AWS 。
   - [Instance information (インスタンス情報)] - OS 名やバージョン、ドメイン、ファイアウォールのステータスなどの情報。
   - [Network configuration (ネットワーク設定) - IP アドレス、ゲートウェイ、サブネットマスクなどの設定情報。
   - [Windows Update (Windows 更新プログラム)] - マネージドインスタンスの Windows 更新プログラムのリスト (Windows インスタンスのみ)。

   > **Note**
   >
   > AWS Config 現時点では、 はカスタムインベントリタイプの記録をサポートしていません。

インベントリ収集は、System Manager の機能の 1 つです。それらの機能は、[Operations Management (業務管理)]、[Actions & Change (アクションと変更)]、[Instances & Nodes (インスタンスとノード)]、[Shared Resources (共有リソース)] のカテゴリにグループ化されています。詳細については、[What is Systems Manager? (System Managerとは?)]、および AWS Systems Manager ユーザーガイドの [Sysytem Manager Capabilities (Systems Manager の機能)] を参照してください。

によって検出されたリソースの検索 AWS Config

AWS Config コンソール、、および AWS Config API を使用して AWS CLI、削除 AWS Config されたリソースや現在記録されていないリソースなど、 がインベントリを取得または検出したリソースを検索できます。 AWS Config AWS Config は、サポートされているリソースタイプのみを検出します。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。

Looking Up Resources (Console)

AWS Config コンソールでリソースタイプやタグ情報を使用してリソースを検索できます。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. [Resource inventory] (リソースのインベントリ) ページで、検索するリソースの検索オプションを指定します。
   - リソースカテゴリ – すべてのリソースカテゴリを選択するか、結果を AWS リソースのみに絞り込みます。
   - [Resource type] (リソースタイプ) — すべてのリソースタイプを選択するか、フィルターに使用するリソースを選択します。
   - [Compliance] (コンプライアンス) — 準拠、非準拠のいずれかのコンプライアンスステータスでフィルターします。
3. AWS Config は、検索オプションに一致するリソースを一覧表示します。リソースに関する以下の情報を確認できます。
   - [Resource identifier] (リソース識別子) — リソース識別子は、リソース ID またはリソース名 (該当する場合) です。リソース識別子のリンクを選択するとリソースの詳細ページが表示されます。
   - [Resource type] (リソースタイプ) – 該当するリソースのタイプが一覧表示されます。
   - コンプライアンス – ルールに対して AWS Config 評価されたリソースのステータス。

Looking Up Resources (AWS CLI)

を使用して、 AWS Config が検出したリソース AWS CLI を一覧表示できます。

AWS Config service **`list-discovered-resources`**コマンドを使用します。

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
```

```
        }
```

レスポンスで一覧表示されたリソースの設定の詳細を表示するには、`get-resource-config-history` コマンドを使用してリソースタイプと ID を指定します。このコマンドの例と からのレスポンスについては AWS Config、「」を参照してください設定履歴の表示。

Looking up Resources (API)

リソースタイプを指定すると、 はそのタイプのリソースのリソース識別子のリスト AWS Config を返します。詳細については、AWS Config API リファレンスの ResourceIdentifier を参照してください。

ListDiscoveredResources アクションを使用します。

レスポンスで一覧表示されたリソースの設定の詳細を取得するには、GetResourceConfigHistory アクションを使用してリソースタイプと ID を指定します。

を使用した AWS リソースのコンプライアンス情報と評価結果の表示 AWS Config

> **Important**
>
> コンプライアンスステータスを正確に報告するには、`AWS::Config::ResourceCompliance` リソースタイプを記録する必要があります。詳細については、AWS 「リソースの記録」を参照してください。

AWS Config コンソールまたは AWS SDKs を使用して、リソースのコンプライアンス情報と評価結果を表示できます。

トピック

- コンプライアンスの表示 (コンソール)
- コンプライアンス (AWS SDKsの表示

コンプライアンスの表示 (コンソール)

コンプライアンスを確認するには (コンソール)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートするリージョンに設定されていることを確認します。サポートされているリージョンのリストについては、AWS Config の「Amazon Web Services 全般のリファレンスのリージョンとエンドポイント」を参照してください。
3. ナビゲーションペインで、[Resources] (リソース) を選択します。[Resource inventory] (リソースのインベントリ) ページで、リソースカテゴリ、リソースタイプ、およびコンプライアンスステータスでフィルタリングできます。必要に応じて、[Include deleted resources] (削除されたリソースを含める) をクリックします。この表には、リソースタイプのリソース識別子、およびそのリソースのリソースコンプライアンスのステータスが表示されます。リソース識別子とは、リソース ID またはリソース名です。
4. リソース識別子の列からリソースを選択します。
5. [Resource Timeline] (リソースタイムライン) ボタンをクリックします。設定イベント、コンプライアンスイベント、または CloudTrail イベントでフィルターできます。

> **Note**
>
> または、[Resource inventory] (リソースのインベントリ) ページでリソース名を直接クリックすることもできます。[Resource Details] (リソースの詳細) ページからリソースタイムラインにアクセスする場合は、[Resource Timeline] (リソースタイムライン) ボタンを使用します。

また、[Resource inventory] (リソースのインベントリ) ページでリソースを探し、そのコンプライアンス状態を確認することもできます。詳細については、「によって検出されたリソースの検索 AWS Config」を参照してください。

コンプライアンス (AWS SDKsの表示

AWS リソースのコンプライアンス情報を取得するには

次のサンプルコードは、`DescribeComplianceByResource` を使用する方法を説明しています。

CLI

AWS CLI

AWS リソースのコンプライアンス情報を取得するには

次のコマンドは、Config によって記録され、1 つ以上のルールに違反する各 EC2 AWS インスタンスのコンプライアンス情報を返します。

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

出力では、各 CappedCount 属性の値は、リソースが違反するルールの数を示します。例えば、次の出力は、インスタンス i-1a2b3c4d が 2 つのルールに違反していることを示しています。

出力:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
```

```
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeComplianceByResource」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、「COMPLIANT」コンプライアンスタイプの **AWS::SSM::ManagedInstanceInventory** リソースタイプをチェックします。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

出力:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- API の詳細については、「 コマンドレットリファレンス (V4)」のDescribeComplianceByResource」を参照してください。 AWS Tools for PowerShell

Tools for PowerShell V5

例 1: この例では、「COMPLIANT」コンプライアンスタイプの **AWS::SSM::ManagedInstanceInventory** リソースタイプをチェックします。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

出力:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
```

```
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- API の詳細については、「 コマンドレットリファレンス (V5)」のDescribeComplianceByResource」を参照してください。 AWS Tools for PowerShell

AWS リソースのコンプライアンス概要を取得するには

次のサンプルコードは、GetComplianceSummaryByResourceType を使用する方法を説明しています。

CLI

AWS CLI

すべてのリソースタイプのコンプライアンス概要を取得するには

次のコマンドは、非準拠の AWS リソースの数と準拠しているリソースの数を返します。

```
aws configservice get-compliance-summary-by-resource-type
```

出力では、各 CappedCount 属性の値は、準拠または非準拠のリソースの数を示します。

出力:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

特定のリソースタイプのコンプライアンス概要を取得するには

次のコマンドは、準拠していない EC2 インスタンスの数と準拠しているインスタンスの数を返します。

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

出力では、各 CappedCount 属性の値は、準拠または非準拠のリソースの数を示します。

出力:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetComplianceSummaryByResourceType」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: このサンプルは、準拠または非準拠のリソースの数を返し、出力を json に変換します。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
```

```
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- API の詳細については、「 コマンドレットリファレンス (V4)」のGetComplianceSummaryByResourceType」を参照してください。 AWS Tools for PowerShell

Tools for PowerShell V5

例 1: このサンプルは、準拠または非準拠のリソースの数を返し、出力を json に変換します。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- API の詳細については、「 コマンドレットリファレンス (V5)」のGetComplianceSummaryByResourceType」を参照してください。 AWS Tools for PowerShell

AWS リソースの評価結果を取得するには

次のサンプルコードは、`GetComplianceDetailsByResource` を使用する方法を説明しています。

CLI

AWS CLI

AWS リソースの評価結果を取得するには

次のコマンドは、EC2 インスタンス `i-1a2b3c4d` が準拠していない各ルールの評価結果を返します。

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

出力:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
```

```
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetComplianceDetailsByResource」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、指定されたリソースについて次のような結果が出ました。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

出力:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V4)」のGetComplianceDetailsByResource」を参照してください。

Tools for PowerShell V5

例 1: この例では、指定されたリソースについて次のような結果が出ました。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

出力:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
```

```
ResultRecordedTime          : 8/25/2019 11:34:56 PM
ResultToken                 :
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のGetComplianceDetailsByResource」を参照してください。

を使用した AWS リソースのコンプライアンス履歴の表示 AWS Config

> **Important**
>
> `AWS::Config::ResourceCompliance` リソースタイプは、リソースの過去のコンプライアンス結果を保存するために使用されます。このリソースタイプの記録は、Config ルールがリソースを評価したり、コンソールで現在のコンプライアンスステータスを表示したりするためには必要ありません。
>
> 記録`AWS::Config::ResourceCompliance`のみにより、リソースタイムラインで時間の経過に伴うコンプライアンス変更履歴を表示できます。履歴コンプライアンスデータが必要ない場合は、このリソースタイプを除外できます。記録するリソースの選択の詳細については、AWS 「リソースの記録」を参照してください。

AWS Config コンソールで、リソースに対して行われた設定、関係、および変更の数を表示できます。を使用して、リソースの設定履歴を表示できます AWS CLI。

トピック

- コンプライアンス履歴の表示 (コンソール)
- コンプライアンス履歴の表示 (AWS CLI)
- リソースおよびルールのコンプライアンス履歴タイムラインの表示

コンプライアンス履歴の表示 (コンソール)

コンソールを使用したコンプライアンス履歴の表示

[Resource inventory] (リソースのインベントリ) ページでリソースを検索する場合は、リソース識別子の列にあるリソース名または ID をクリックするとリソースの詳細ページが表示されます。詳細ページは、リソースの設定、関係、および変更数の情報を提供します。

[Resource Details] (リソースの詳細) ページからリソースタイムラインにアクセスする場合は、[Resource Timeline] (リソースタイムライン) ボタンを使用します。リソースタイムラインでは、特定のリソースの一定期間の変更を `ConfigurationItems` としてキャプチャします。設定イベント、コンプライアンスイベント、または CloudTrail イベントでフィルターできます。

コンプライアンス履歴の表示 (AWS CLI)

を使用したコンプライアンス履歴の表示 AWS CLI

が AWS Config 記録する設定項目は、設定スナップショットおよび設定ストリームとして、オンデマンドで指定された配信チャネルに配信されます。を使用して AWS CLI 、各リソースの設定項目の履歴を表示できます。

設定履歴の表示

`get-resource-config-history` コマンドを入力し、リソースタイプおよびリソース ID を指定します。以下に例を示します。

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
```

```
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

レスポンスフィールドの詳しい説明については、「Components of a Configuration Item」および「でサポートされているリソースタイプ AWS Config」を参照してください。

AWS Configからの Amazon EBS 設定履歴の例

AWS Config は、それぞれがリソースタイプを表す一連のファイルを生成し、記録するそのタイプのリソースのすべての設定変更を一覧表示します。 AWS Config AWS Config は、このリソース中心の設定履歴を、有効にしたときに指定した Amazon S3 バケット内のオブジェクトとしてエクスポートします AWS Config。リソースタイプごとの設定履歴ファイルには、最後の履歴ファイルの配信後

に、このタイプのリソースで検出された変更が含まれています。通常、履歴ファイルは 6 時間ごとに配信されます。

次の例では、 AWS アカウントの現在のリージョンで、すべての Amazon Elastic Block Store ボリュームの設定履歴を記述する Amazon S3 オブジェクトの内容を示します。このアカウントのボリュームには `vol-ce676ccc` と `vol-cia007c` が含まれています。前回の履歴ファイルの配信後に、ボリューム `vol-ce676ccc` には 2 つの設定変更があり、ボリューム `vol-cia007c` には 1 つの設定変更があります。

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
```

```
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-ad229edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04w292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
```

```
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-cia007c",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
```

```
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

リソースおよびルールのコンプライアンス履歴タイムラインの表示

AWS Config は、 によって評価されるリソースのコンプライアンス状態の変更の保存をサポートします AWS Config ルール。リソースのコンプライアンス履歴は、タイムラインの形式で表示されます。タイムラインでは、特定リソースの一定期間の変更を `ConfigurationItems` としてキャプチャします。の内容の詳細については`ConfigurationItem`、 AWS Config API リファレンスの[ConfigurationItem](#)」を参照してください。

AWS Configのすべてのリソースタイプの記録をオプトインまたはオプトアウトすることができます。すべてのリソースタイプを記録することを選択した場合、 は によって評価されたリソースコンプライアンス履歴 AWS Config の記録を自動的に開始します AWS Config ルール。デフォルトでは、はサポートされているすべてのリソースの設定変更 AWS Config を記録します。また、リソースコンプライアンス履歴の特定のリソースタイプ (`AWS::Config::ResourceCompliance`) のみを選択することもできます。詳細については、[AWS 「レコードの記録](#)」を参照してください。

Viewing Resource Timeline Using Resources

[Resource inventory] (リソースのインベントリ) ページから特定のリソースを選択して、リソースのタイムラインにアクセスします。

1. ナビゲーションから、[Resources] (リソース)をクリックします。
2. [Resource inventory] (リソースのインベントリ) ページで、リソースカテゴリ、リソースタイプ、およびコンプライアンスステータスでフィルタリングできます。必要に応じて、[Include deleted resources] (削除されたリソースを含める) をクリックします。

   この表には、リソースタイプのリソース識別子、およびそのリソースのリソースコンプライアンスのステータスが表示されます。リソース識別子とは、リソース ID またはリソース名です。
3. リソース識別子の列からリソースを選択します。
4. [Resource Timeline] (リソースタイムライン) ボタンをクリックします。設定イベント、コンプライアンスイベント、または CloudTrail イベントでフィルターできます。

> **Note**
>
> または、[Resource inventory] (リソースのインベントリ) ページでリソース名を直接クリックすることもできます。[Resource Details] (リソースの詳細) ページからリソースタイムラインにアクセスする場合は、[Resource Timeline] (リソースタイムライン) ボタンを使用します。

Viewing Resource Timeline Using Rules

[Rule] (ルール) ページから特定のルールを選択して、リソースタイムラインにアクセスします。

1. 左のナビゲーションから [Rules] を選択します。
2. [Rule] (ルール) ページで、関連するリソースを評価しているルールの名前をクリックします。ルールが画面に表示されない場合は、[Add rule] ボタンを使用してルールを追加します。
3. ルールの詳細ページで、評価が行われたリソースの表からリソースを選択します。
4. [Resource Timeline] (リソースタイムライン) ボタンをクリックします。リソースのタイムラインが表示されます。

AWS リソースのコンプライアンス履歴のクエリ

get-resource-config-history を使用して、リソースタイプ `AWS::Config::ResourceCompliance` でリソースコンプライアンス履歴の問い合わせを行います。

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

次のような出力が表示されます:

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
     "relationshipName": "Is associated with "
    }
   ]
   "tags": {},
   "resourceType": "AWS::Config::ResourceCompliance",
   "resourceId": "AWS::S3::Bucket/configrules-bucket",
   "ConfigurationStateId": "1539799966921",
   "relatedEvents": [];
   "awsRegion": "us-west-2",
   "version": "1.3",
   "configurationItemMD5Hash": "",
```

```
    "supplementaryConfiguration": {},
    "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

    "configurationItemStatus": "ResourceDiscovered",
    "accountId": "AccountID"
   }
  ]
}
```

AWS Config リソースのタグ付け

タグは、 AWS リソースに割り当てるラベルです。タグはそれぞれ、1 つのキーとオプションの 1 つの値で構成されており、どちらもお客様側が定義します。タグを使用することで、リソースの管理、検索、フィルタリングを行うことができます。

タグを使用すると、 AWS リソースを目的、所有者、環境などさまざまな方法で分類できます。これは、同じタイプのリソースが多数ある場合に役立ちます。割り当てたタグに基づいて特定のリソースをすばやく識別できます。 AWS リソースには 1 つ以上のタグを割り当てることができます。各タグには値も関連付けられています。

各リソースタイプのニーズを満たす一連のタグキーを考案することをお勧めします。一貫性のあるタグキーのセットを使用することで、 AWS リソースの管理が容易になります。追加したタグに基づいてリソースを検索およびフィルタリングできます。

タグは厳密に文字列として解釈され、自動的にリソースに割り当てられることはありません。タグのキーと値は編集でき、タグはリソースからいつでも削除できます。タグの値を空の文字列に設定することはできますが、タグの値を null に設定することはできません。特定のリソースについて既存のタグと同じキーを持つタグを追加した場合、以前の値は新しい値によって上書きされます。リソースを削除すると、リソースのタグも削除されます。

AWS Command Line Interface（AWS CLI) と AWS Config API リファレンスを使用してタグを操作できます。

タグ付けに関連する制限

タグには以下のような基本制限があります。

制限	説明
リソースあたりのタグの最大数	50
キーの最大長	UTF-8 で 128 文字の Unicode 文字
値の最大長	UTF-8 で 256 文字の Unicode 文字
プレフィックスの制限	タグ名または値に `aws:` プレフィックスを使用しないでください。このプレフィックスは AWS 用に予約されています。このプレフィックスが含まれるタグの名前または値は編集または削除できません。このプレフィックスを持つタグは、リソースあたりのタグ数の制限時には計算されません。
文字の制限	タグに使用できるのは、Unicode 文字、数字、空白、または `_ . : / = + - @` のみです。

AWS Config API アクションによるタグの管理

タグベースのアクセスコントロールは、3 つのリソース `ConfigurationAggregator`、`AggregationAuthorization`、`ConfigRule` で利用できます。リソースのタグの追加、更新、リスト表示、および削除には、次を使用します。

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResource` アクセスを制御するには、特定の AWS Identity and Access Management (IAM) アクセス許可`UntagResource`が必要です。詳細については、IAM ユーザーガイドのタグキーに基づいたアクセス制御を参照してください。

AWS Config ルールを使用したリソースの評価

を使用して AWS Config 、 AWS リソースの設定を評価します。これを行うには、最適な構成設定を表す AWS Config ルールを作成します。 は、 マネージドルールと呼ばれるカスタマイズ可能な事前定義されたルール AWS Config を提供し、使用開始を支援します。

トピック

- 考慮事項
- リージョンのサポート
- AWS Config ルールのコンポーネント
- AWS Config マネージドルール
- AWS Config カスタムルール
- サービスにリンクされた AWS Config ルール
- 組織内のすべてのアカウントでの AWS Config ルールの管理
- AWS Config ルールの追加
- AWS Config ルールの更新
- AWS Config ルールの削除
- AWS Config ルールの詳細とコンプライアンス情報の表示
- AWS Config ルールのプロアクティブ評価を有効にする
- ルール評価を Security Hub に送信する
- AWS Config ルールを使用したリソースの評価
- AWS Config ルールから評価結果を削除する
- AWS Config ルールのトラブルシューティング

考慮事項

Cost Considerations

リソースの記録に関連するコストの詳細については、「AWS Config の料金」を参照してください。

推奨事項: ルールを削除する前に**`AWS::Config::ResourceCompliance`**、リソースタイプを記録から除外することを検討してください。

ルールを削除するCIs) が作成されます。 `AWS::Config::ResourceCompliance`多数のリソースタイプを評価するルールを削除すると、記録された CI の数が増加する可能性があります。

関連するコストを回避するには、ルールを削除する前に`AWS::Config::ResourceCompliance`リソースタイプの記録を無効にし、ルールが削除された後に記録を再度有効にすることを選択できます。

ただし、ルールの削除は非同期プロセスであるため、完了までに 1 時間以上かかる場合があります。の記録が無効になっている間`AWS::Config::ResourceCompliance`、ルール評価は関連するリソースの履歴には記録されません。

AWS Config では、ルールの削除方法を決定する前に、これらの要因をcase-by-caseで比較検討することをお勧めします。

推奨事項: カスタム Lambda ルールの削除済みリソースの評価を処理するロジックを追加します

AWS Config カスタム Lambda ルールを作成するときは、削除されたリソースの評価を処理するロジックを追加することを強くお勧めします。

評価結果が `NOT_APPLICABLE` としてマークされている場合、削除およびクリーンアップの対象としてマークされます。`NOT_APPLICABLE` としてマークされていない場合は、ルールが削除されるまで評価結果が変更されないため、ルールの削除時に `AWS::Config::ResourceCompliance` の CI の作成が予想以上に急増する可能性あります。

削除されたリソース`NOT_APPLICABLE`を返すように AWS Config カスタム Lambda ルールを設定する方法については、AWS Config 「カスタム Lambda ルールを使用した削除されたリソースの管理」を参照してください。

推奨事項: カスタム Lambda ルールの対象となるリソースを提供します

AWS Config ルールが 1 つ以上のリソースタイプにスコープされていない場合、カスタム Lambda ルールは多数の Lambda 関数呼び出しを引き起こす可能性があります。アカウントに関連するアクティビティの増加を回避するには、カスタム Lambda ルールの対象範囲内のリソースを提供することを強く推奨します。リソースタイプが選択されていない場合、そのルールによってアカウント内のすべてのリソースの Lambda 関数を呼び出します。

Other considerations

マネージドルールのデフォルト値

マネージドルールに指定されたデフォルト値は、 AWS コンソールを使用する場合にのみ事前入力されます。デフォルト値が API、CLI、または SDK に自動設定されることはありません。

設定項目の記録遅延

AWS Config 通常、 は、変更が検出された直後、または指定した頻度でリソースの設定変更を記録します。ただし、これはベストエフォートベースであり、場合によっては時間がかかることがあります。たとえば、既知の遅延があるリソースタイプは ですAWS::SecretsManager::Secret。このリソースタイプは例であり、このリストは網羅的ではありません。

ポリシーとコンプライアンス結果

で管理される IAM ポリシーやその他のポリシーは、 AWS Config がリソースの設定変更を記録するアクセス許可を持っているかどうかに影響を与える可能性があります。 AWS Organizationsさらに、ルールはリソースの設定を直接評価し、ルールは評価の実行時にこれらのポリシーを考慮しません。有効なポリシーが、 の使用方法と一致していることを確認してください AWS Config。

リソースタイプのタグ付けのサポート

リソースタイプがタグ付けをサポートしていない場合、または describe API レスポンスにタグ情報が含まれていない場合、そのリソースタイプの設定項目 (CIs) AWS Config にタグデータはキャプチャされません。 AWS Config は引き続きこれらのリソースを記録します。ただし、タグデータに依存する機能は機能しません。これは、タグデータに依存するタグベースのフィルタリング、グループ化、またはコンプライアンス評価に影響します。

ディレクトリバケットはサポートされていません

マネージドルールは、Amazon Simple Storage Service (Amazon S3) リソースを評価するときにのみ汎用バケットをサポートします。汎用バケットとディレクトリバケットの詳細については、「Amazon S3 ユーザーガイド」の「バケットの概要」と「ディレクトリバケット」を参照してください。

マネージドルールとグローバル IAM リソースタイプ

2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (AWS::IAM::Group、AWS::IAM::Policy、AWS::IAM::Role、および AWS::IAM::User) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降に でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。

少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。

不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

リージョンのサポート

現在、 AWS Config ルール機能は以下の AWS リージョンでサポートされています。どのリージョンで個々の AWS Config ルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
米国西部 (北カリフォルニア)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
アジアパシフィック (ハイデラバード)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
アジアパシフィック (マレーシア)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
アジアパシフィック (台北)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
アジアパシフィック (タイ)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
メキシコ (中部)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS 組織のメンバーアカウント間での AWS Config ルールのデプロイは、次のリージョンでサポートされています。

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
米国西部 (北カリフォルニア)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
アジアパシフィック (ハイデラバード)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config ルールのコンポーネント

AWS Config ルールは、 AWS リソースの設定を評価します。このページでは、ルールのコンポーネントについて説明します。

トピック

- AWS Config ルールの仕組み
- トリガータイプ
- 評価モード
- AWS Config ルールメタデータ

AWS Config ルールの仕組み

AWS Config はリソース間で発生する設定変更を継続的に追跡し、これらの変更がルールの条件に不適合になっていないかどうかを確認します。リソースがルールに準拠していない場合、 はリソースとルールを非準拠として AWS Config フラグ付けします。

AWS Config ルールには 4 つの評価結果があります。

評価結果	説明
`COMPLIANT`	ルールはコンプライアンスチェックの条件に合格します。
`NON_COMPLIANT`	ルールはコンプライアンスチェックの条件に失敗します。
`ERROR`	必須/オプションのパラメータの 1 つが無効であるか、正しいタイプではないか、形式が正しくありません。
`NOT_APPLICABLE`	ルールのロジックを適用できないリソースを除外するために使用されます。例えば、alb-desync-mode-check ルールは Application Load Balancer のみをチェックし、Network Load Balancer と Gateway Load Balancer は無視します。

たとえば、EC2 ボリュームを作成すると、 はボリュームを暗号化する必要があるルールに照らしてボリュームを評価 AWS Config できます。ボリュームが暗号化されていない場合、 はボリュームとルールを非準拠として AWS Config フラグ付けします。 AWS Config は、アカウント全体の要件についてすべてのリソースを確認することもできます。たとえば、 AWS Config は、アカウント内の EC2 ボリュームの数が希望する合計数内に収まっているかどうか、またはアカウントがログ AWS CloudTrail 記録に を使用しているかどうかを確認できます。

トリガータイプ

アカウントにルールを追加すると、 はリソースをルールの条件 AWS Config と比較します。この最初の評価の後、 は評価がトリガーされるたびに評価の実行を AWS Config 続行します。評価のトリガーは、ルールの一部として定義されます。以下のタイプを含めることができます。

トリガータイプ	説明
設定変更	AWS Config は、ルールのスコープに一致するリソースがあり、リソースの設定が変更された場合に、ルールの評価を実行します。評価は、が設定項目の変更通知 AWS Config を送信した後に実行されます。 どのリソースで評価を開始するかは、ルールのスコープで定義します。スコープには以下を含めることができます。 • 1 つ以上のリソースタイプ • リソースタイプとリソース ID の組み合わせ • タグキーとタグ値の組み合わせ • 記録対象リソースの作成、更新、または削除時 AWS Config は、ルールのスコープに一致するリソースへの変更を検出すると、評価を実行します。スコープを使用して評価を開始するリソースを定義できます。
定期的	AWS Config は、24 時間ごとなど、選択した頻度でルールの評価を実行します。
ハイブリッド	一部のルールでは、設定変更と定期的なトリガーの両方があります。これらのルールでは、は、設定の変更を検出したときと、指定した頻度でリソース AWS Config を評価します。

評価モード

AWS Config ルールには 2 つの評価モードがあります。

評価モード	説明
プロアクティブ	プロアクティブ評価は、デプロイ前のリソースを評価するために使用します。これにより、リージョンのアカウントにあるプロアクティブルールのセットを考慮すると、 AWS リソースを定義するためにリソースプロパティのセットが COMPLIANT か NON_COMPLIANT かを評価できます。
検出	検出評価は、デプロイ済みのリソースを評価するために使用します。これにより、既存のリソース構成の設定を評価できます。

> **Note**
>
> プロアクティブルールは、NON_COMPLIANT のフラグが付けられたリソースを修正したり、これらのリソースのデプロイを妨げたりしません。

詳細については、AWS Config 「ルールのプロアクティブ評価を有効にする」を参照してください。

プロアクティブ評価によるマネージドルールのリスト

プロアクティブ評価をサポートするマネージドルールのリストについては、「評価モード別の AWS Config マネージドルールのリスト」を参照してください。

プロアクティブ評価がサポートされているリソースタイプのリスト

プロアクティブ評価がサポートされているリソースタイプのリストを以下に示します。

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`

- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

AWS Config ルールメタデータ

AWS Config ルールには、次の変更可能なメタデータを含めることができます。

defaultName

defaultName は、ルールのインスタンスがデフォルトで取得する名前です。

[Description] (説明)

ルールの説明は、ルールが評価する内容のコンテキストを提供します。 AWS Config コンソールには 256 文字の制限があります。ベストプラクティスとして、ルールの説明に「するかどうかを確認」で始まる、NON_COMPLIANT シナリオの説明を含めます。サービス名は、ルールの説明で最初に言及されたときに、 AWS または Amazon で始まる完全な形で記述する必要があります。例えば、 AWS CloudTrail CloudTrail や Amazon CloudWatch の代わりに Amazon CloudWatch を初めて使用する場合などです。それ以降に言及するときは、サービス名を省略できます。

scope

スコープは、ルールがターゲットとするリソースタイプを決定します。サポートされるリソースタイプのリストについては、サポートされているリソースタイプを参照してください。

compulsoryInputParameterDetails

compulsoryInputParameterDetails は、ルールが評価を行うために必要なパラメータに使用されます。例えば、`access-keys-rotated` マネージドルールには、必須パラメータとして `maxAccessKeyAge` が含まれます。パラメータが必須の場合、(オプション) としてマークさ

れません。パラメータごとに、型を指定する必要があります。型は、「String」、「int」、「double」、「CSV」、「boolean」、「StringMap」のいずれかになります。

optionalInputParameterDetails

OptionalInputParameterDetails は、ルールが評価を行うためのオプションのパラメータに使用されます。例えば、`elasticsearch-logs-to-cloudwatch` マネージドルールには、オプションのパラメータとして `logTypes` が含まれます。パラメータごとに、型を指定する必要があります。型は、「String」、「int」、「double」、「CSV」、「boolean」、「StringMap」のいずれかになります。

supportedEvaluationModes

supportedEvaluationModes は、リソースをデプロイ前またはデプロイ後のいずれで評価するかを決定します。

`DETECTIVE` は、デプロイ済みのリソースを評価するために使用します。これにより、既存のリソース構成設定を評価できます。`PROACTIVE` は、リソースをデプロイ前に評価するために使用します。

これにより、 リージョンのアカウントにあるプロアクティブルールのセットを考慮すると、 AWS リソースを定義するためにリソースプロパティのセットが COMPLIANT か NON_COMPLIANT かを評価できます。

supportedEvaluationModes は `DETECTIVE`、`PROACTIVE`、または `DETECTIVE` と `PROACTIVE` の両方に指定できます。評価モードは指定する必要があり、このフィールドを空のままにすることはできません。

> **Note**
>
> プロアクティブルールは、NON_COMPLIANT のフラグが付けられたリソースを修正したり、これらのリソースのデプロイを妨げたりしません。

AWS Config マネージドルール

AWS Config には、 AWS マネージドルールが用意されています。マネージドルールは、 が AWS リソースが一般的なベストプラクティスに準拠しているかどうかを評価するために AWS Config 使用する、事前定義されたカスタマイズ可能なルールです。例えば、マネージドルールを使用すると、Amazon Elastic Block Store (Amazon EBS) ボリュームが暗号化されているかどうか、または特定のタグがリソースに適用されているかどうかの評価をすぐに開始できます。

AWS Config コンソールでは、マネージドルールを設定およびアクティブ化するプロセスについて説明します。 AWS Command Line Interface または AWS Config API を使用して、マネージドルールの設定を定義する JSON コードを渡すこともできます。

マネージドルールの動作は、ニーズに合わせてカスタマイズできます。例えば、ルールの評価をトリガーするリソースを EC2 インスタンスやボリュームなどに制限するようにルールのスコープを定義できます。

ルールのパラメータをカスタマイズして、ルールに準拠するためにリソースに必要とされる属性を定義できます。例えば、パラメータをカスタマイズして、特定のポート番号に着信するトラフィックをセキュリティグループでブロックするように指定できます。

マネージドルールを使用する前に、「」を参照してください考慮事項。

トピック

- AWS Config マネージドルールのリスト
- 評価モード別の AWS Config マネージドルールのリスト
- トリガータイプ別の AWS Config マネージドルールのリスト
- リージョンの可用性別の AWS Config マネージドルールのリスト
- AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成

AWS Config マネージドルールのリスト

AWS Config は現在、次の マネージドルールをサポートしています。これらのルールを使用する前に、「」を参照してください考慮事項。

トピック

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description

- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された Aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリポイント暗号化
- バックアップ/リカバリポイントの手動削除/無効化
- バックアップ/リカバリポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled

- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled

- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled

- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- DynamoDB-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-systems-manager
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged

- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache_automatic_backup_check_enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions

- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- iam-server-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- restricted-ssh
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- ec2-instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged

- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き

- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication

- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch

- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch

- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access

- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

access-keys-rotated

アクティブな IAM アクセスキーが、`maxAccessKeyAge` で指定された日数内にローテーション (変更) されるかどうかを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

> **Warning**
>
> アカウント識別子を確認するためであっても、アクセスキーを認可されていない当事者に提供しないでください。提供すると、第三者がアカウントへの永続的なアクセスを取得する場合があります。セキュリティ保護のためのベストプラクティスは、ユーザーがパスワードやアクセスキーを使用しなくなったら、それらを削除することです。

> **Note**
>
> コンソールで非準拠としてマークされたリソースタイプ
> このルールにより、いずれかのアクセスキーが非準拠であることが判明した場合、`AWS::IAM::User`リソースタイプも AWS コンソールで非準拠としてマークされます。
> マネージドルールとグローバル IAM リソースタイプ

2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および `AWS::IAM::User`) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降、 でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。
少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。
制約事項
このルールは、 AWS アカウントのルートユーザーアクセスキーには適用されません。ルートユーザーアクセスキーを削除またはローテーションするには、ルートユーザーの認証情報を使用して、 AWS Management Console の「My Security Credentials」ページにサインインしますhttps://aws.amazon.com/console/。

識別子: ACCESS_KEYS_ROTATED

リソースタイプ: AWS::IAM::User

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

maxAccessKeyAge, タイプ: int, デフォルト: 90

ローテーションなしの最大日数。デフォルト: 90

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

account-part-of-organizations

AWS アカウントが AWS Organizations の一部であるかどうかを確認します。 AWS アカウントが AWS Organizations の一部でない場合、または AWS Organizations マスターアカウント ID がルールパラメータ と一致しない場合、ルールは NON_COMPLIANT ですMasterAccountId。

> **Note**
>
> マネージドルールとグローバル IAM リソースタイプ
> 2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (AWS::IAM::Group、AWS::IAM::Policy、AWS::IAM::Role、および AWS::IAM::User) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降に でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。
> 少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
> 不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

識別子: ACCOUNT_PART_OF_ORGANIZATIONS

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (台北) AWS を除くサポートされているすべての リージョン

パラメータ：

MasterAccountId (オプション), タイプ: 文字列

アカウントのマスター AWS アカウント ID。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

acmpca-certificate-authority-tagged

AWS プライベート CA 認証機関にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： ACMPCA_CERTIFICATE_AUTHORITY_TAGGED

リソースタイプ: AWS::ACMPCA::CertificateAuthority

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京）、アジアパシフィック (タイ）、アジアパシフィック (マレーシア）、 AWS GovCloud (米国東部）、 AWS GovCloud (米国西部）、メキシコ (中部）、アジアパシフィック (台北）、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション）, タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

acm-certificate-expiration-check

アカウントの AWS Certificate Manager 証明書が、指定された日数内に有効期限としてマークされているかどうかを確認します。ACM が提供する証明書は自動的に更新されます。ACM は、ユーザーがインポートした証明書を自動的に更新しません。証明書の有効期限が近づいている場合、ルールは NON_COMPLIANT です。

識別子: ACM_CERTIFICATE_EXPIRATION_CHECK

リソースタイプ: AWS::ACM::Certificate

トリガータイプ: 設定変更および定期的

AWS リージョン： アジアパシフィック (大阪) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

daysToExpiration (オプション), タイプ: int, デフォルト: 14

ルールで ACM 証明書を非準拠としてフラグ付けするまでの日数を指定します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

acm-certificate-rsa-check

AWS Certificate Manager (ACM) によって管理される RSA 証明書のキー長が '2048' ビット以上であるかどうかを確認します。最小キー長が 2048 ビット未満の場合、ルールは NON_COMPLIANT です。

識別子: ACM_CERTIFICATE_RSA_CHECK

リソースタイプ: AWS::ACM::Certificate

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシ

フィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

acm-pca-root-ca-disabled

Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっているかどうかを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

識別子: ACM_PCA_ROOT_CA_DISABLED

リソースタイプ: AWS::ACMPCA::CertificateAuthority

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

exemptedCAArns (オプション), タイプ: CSV

有効にできる CA の Amazon リソースネーム (ARN) のカンマ区切りリスト。この値は、特定のルート CA や有効にできる中間 CA など、他の CA にも指定できます。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

active-mq-supported-version

Amazon MQ ActiveMQ ブローカーが、指定された最小サポートエンジンバージョンで実行されているかどうかを確認します。ActiveMQ ブローカーが、指定したサポートされている最小エンジンバージョンで実行されていない場合、ルールは NON_COMPLIANT です。

識別子: ACTIVE_MQ_SUPPORTED_VERSION

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

supportedEngineVersion, タイプ: 文字列

> ActiveMQ ブローカーでサポートされている最小エンジンバージョンをチェックするルールの文字列値。ActiveMQ ブローカーはセマンティックバージョニング仕様を使用します。X.Y.Z. X はメジャーバージョン、Y はマイナーバージョン、Z はパッチバージョンを表します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

alb-desync-mode-check

Application Load Balancer (ALB) がユーザー定義の desync 軽減モードで設定されているかどうかを確認します。ALB desync 軽減モードがユーザー定義の desync 軽減モードと一致しない場合、ルールは NON_COMPLIANT です。

識別子: ALB_DESYNC_MODE_CHECK

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

desyncMode, タイプ: CSV

カンマ区切りのリスト。「defensive」、「strictest」、「monitor」から最大 2 つの値を選択できます。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

alb-http-drop-invalid-header-enabled

ルールが AWS Application Load Balancer (ALB) を評価して、http ヘッダーを削除するように設定されているかどうかを確認します。routing.http.drop_invalid_header_fields.enabled の値が false に設定されている場合、ルールは NON_COMPLIANT です。

識別子: ALB_HTTP_DROP_INVALID_HEADER_ENABLED

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (大阪) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

alb-http-to-https-redirection-check

HTTP から HTTPS へのリダイレクトが Application Load Balancer のすべての HTTP リスナーで設定されているかどうかを確認します。Application Load Balancer の 1 つまたは複数の HTTP リスナーに HTTP から HTTPS へのリダイレクトが設定されていない場合、ルールは NON_COMPLIANT です。また、1 つ以上の HTTP リスナーが、リダイレクトではなく HTTP リスナーへの転送を行っている場合、ルールは NON_COMPLIANT となります。

識別子: ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (大阪) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

alb-internal-scheme-check

Application Load Balancer スキームが内部的かどうかを確認します。configuration.scheme が内部に設定されていない場合、ルールは NON_COMPLIANT です。

識別子： ALB_INTERNAL_SCHEME_CHECK

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

alb-listener-tagged

Application Load Balancer リスナーにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： ALB_LISTENER_TAGGED

リソースタイプ： AWS::ElasticLoadBalancingV2::Listener

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

alb-waf-enabled

Application Load Balancer (ALBs) で AWS WAF が有効になっているかどうかを確認します。key: waf.enabled が false に設定されている場合、ルールは NON_COMPLIANT です。

識別子: ALB_WAF_ENABLED

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (大阪) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

wafWebAclIds (オプション), タイプ: CSV

ALB の関連付けを確認するウェブ ACL ID (WAF の場合) またはウェブ ACL ARN (WAFV2 の場合) のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

amplify-app-branch-auto-deletion-enabled

Git リポジトリからブランチを削除するときに AWS 、Amplify アプリが Amplify ホスティングのブランチを自動的に切断するかどうかを確認します。configuration.EnableBranchAutoDeletion が false の場合、ルールは NON_COMPLIANT です。

識別子： AMPLIFY_APP_BRANCH_AUTO_DELETION_ENABLED

リソースタイプ： AWS::Amplify::App

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

amplify-app-description

Amplify AWS アプリに説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： AMPLIFY_APP_DESCRIPTION

リソースタイプ： AWS::Amplify::App

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

amplify-app-tagged

Amplify AWS アプリにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： AMPLIFY_APP_TAGGED

リソースタイプ： AWS::Amplify::App

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

amplify-branch-performance-mode-enabled

Amplify AWS ブランチでパフォーマンスモードが有効になっているかどうかを確認します。configuration.EnablePerformanceMode が false の場合、ルールは NON_COMPLIANT です。

識別子： AMPLIFY_BRANCH_PERFORMANCE_MODE_ENABLED

リソースタイプ： AWS::Amplify::Branch

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

amplify-branch-tagged

Amplify AWS ブランチにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： AMPLIFY_BRANCH_TAGGED

リソースタイプ： AWS::Amplify::Branch

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバー

ド) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

api-gwv2-access-logs-enabled

Amazon API Gateway V2 ステージで、アクセスログが有効かどうかを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。

識別子: API_GWV2_ACCESS_LOGS_ENABLED

リソースタイプ: AWS::ApiGatewayV2::Stage

トリガータイプ: 設定変更

AWS リージョン : アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべてのリージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

api-gwv2-authorization-type-configured

Amazon API Gatewayv2 API ルートに認可タイプが設定されているかどうかを確認します。認可タイプが NONE の場合、ルールは NON_COMPLIANT です。

識別子: API_GWV2_AUTHORIZATION_TYPE_CONFIGURED

リソースタイプ: AWS::ApiGatewayV2::Route

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべてのリージョン

パラメータ :

認証タイプ (オプション), タイプ: 文字列

> API ルートの認可タイプを確認するパラメータです。CUSTOM、 AWS_IAM、JWT に一致する文字列パラメータは有効です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

api-gw-associated-with-waf

Amazon API Gateway API ステージが AWS WAF ウェブアクセスコントロールリスト (ウェブ ACL) を使用しているかどうかを確認します。 AWS WAF ウェブ ACL が使用されていない場合、または

使用されている AWS ウェブ ACL がルールパラメータにリストされているものと一致しない場合、ルールは NON_COMPLIANT です。

識別子: API_GW_ASSOCIATED_WITH_WAF

リソースタイプ: AWS::ApiGateway::Stage

トリガータイプ: 設定変更

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

WebAclArns (オプション), タイプ: CSV

ウェブ ACL Amazon リソースネーム (ARN) のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

api-gw-cache-enabled-and-encrypted

Amazon API Gateway ステージのすべてのメソッドでキャッシュが有効になっているか、および暗号化されているかどうかを確認します。Amazon API Gateway ステージのいずれかのメソッドでキャッシュが設定されていない場合、またはキャッシュが暗号化されていない場合、ルールは NON_COMPLIANT です。

識別子: API_GW_CACHE_ENABLED_AND_ENCRYPTED

リソースタイプ: AWS::ApiGateway::Stage

トリガータイプ: 設定変更

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

api-gw-endpoint-type-check

Amazon API Gateway の API がルールパラメータ `endpointConfigurationType` で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。

識別子: API_GW_ENDPOINT_TYPE_CHECK

リソースタイプ: AWS::ApiGateway::RestApi

トリガータイプ: 設定変更

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

endpointConfigurationTypes, 型: 文字列

許可される endpointConfigurationTypes のカンマ区切りリスト。使用できる値は REGIONAL、PRIVATE、EDGE です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

api-gw-execution-logging-enabled

Amazon API Gateway ステージのすべてのメソッドのログ記録が有効になっているかどうかを確認します。ログ記録が有効にされていない場合、または `loggingLevel` が ERROR でも INFO でもない場合、ルールは NON_COMPLIANT です。

識別子: API_GW_EXECUTION_LOGGING_ENABLED

リソースタイプ: AWS::ApiGateway::Stage、AWS::ApiGatewayV2::Stage

トリガータイプ: 設定変更

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

loggingLevel (オプション), 型: 文字列, デフォルト: ERROR、INFO

(オプション) 特定のログ記録レベルのカンマ区切りリスト (例: ERROR, INFO、または ERROR,INFO)。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

api-gw-ssl-enabled

REST API ステージで SSL 証明書が使用されるかどうかを確認します。REST API ステージに関連する SSL 証明書がない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> GetIntegration API が type として `AWS` を返した場合、このルールでは `NOT_APPLICABLE` を返します。

識別子: API_GW_SSL_ENABLED

リソースタイプ: AWS::ApiGateway::Stage

トリガータイプ: 設定変更

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

CertificateIDs (オプション), タイプ: CSV

REST API ステージで設定されたクライアント証明書 ID のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

api-gw-xray-enabled

Amazon API Gateway REST API で AWS X-Ray トレースが有効になっているかどうかを確認します。 APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

識別子: API_GW_XRAY_ENABLED

リソースタイプ: AWS::ApiGateway::Stage

トリガータイプ: 設定変更

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、[AWS Config 「ルールを使用したリソースの評価](#)」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、[StartResourceEvaluation](#) API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
```

```
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

appconfig-application-description

AWS AppConfig アプリケーションに説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： APPCONFIG_APPLICATION_DESCRIPTION

リソースタイプ： AWS::AppConfig::Application

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

appconfig-application-tagged

AWS AppConfig アプリケーションにタグがあるかどうかを確認します。必要に応じて、チェックするルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPCONFIG_APPLICATION_TAGGED

リソースタイプ： AWS::AppConfig::Application

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appconfig-configuration-profile-tagged

AWS AppConfig 設定プロファイルにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPCONFIG_CONFIGURATION_PROFILE_TAGGED

リソースタイプ： AWS::AppConfig::ConfigurationProfile

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appconfig-configuration-profile-validators-not-empty

AWS AppConfig 設定プロファイルに構文チェックまたはセマンティックチェック用の検証子が少なくとも 1 つ含まれているかどうかをチェックして、設定デプロイが意図したとおりに機能することを確認します。Validators プロパティが空の配列の場合、ルールは NON_COMPLIANT です。

識別子： APPCONFIG_CONFIGURATION_PROFILE_VALIDATORS_NOT_EMPTY

リソースタイプ： AWS::AppConfig::ConfigurationProfile

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

appconfig-deployment-strategy-description

AWS AppConfig デプロイ戦略に説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： APPCONFIG_DEPLOYMENT_STRATEGY_DESCRIPTION

リソースタイプ： AWS::AppConfig::DeploymentStrategy

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

appconfig-deployment-strategy-replicate-to-ssm

AWS AppConfig デプロイ戦略がデプロイ戦略を AWS Systems Manager (SSM) ドキュメントに保存しているかどうかを確認します。configuration.ReplicateTo が 'SSM_DOCUMENT' でない場合、ルールは NON_COMPLIANT です。

識別子： APPCONFIG_DEPLOYMENT_STRATEGY_REPLICATE_TO_SSM

リソースタイプ： AWS::AppConfig::DeploymentStrategy

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appconfig-environment-description

AWS AppConfig 環境の説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： APPCONFIG_ENVIRONMENT_DESCRIPTION

リソースタイプ： AWS::AppConfig::Environment

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appconfig-environment-tagged

AWS AppConfig 環境にタグがあるかどうかを確認します。必要に応じて、チェックするルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPCONFIG_ENVIRONMENT_TAGGED

リソースタイプ： AWS::AppConfig::Environment

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appconfig-extension-association-tagged

AWS AppConfig 拡張機能の関連付けにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPCONFIG_EXTENSION_ASSOCIATION_TAGGED

リソースタイプ： AWS::AppConfig::ExtensionAssociation

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appconfig-freeform-profile-config-storage

AWS AppConfig のフリーフォーム設定プロファイルが、設定データを AWS Secrets Manager または AWS AppConfig ホスト設定ストアに保存しているかどうかを確認します。configuration.LocationUri が secretsmanager またはホストされていない場合、ルールは NON_COMPLIANT です。

識別子： APPCONFIG_FREEFORM_PROFILE_CONFIG_STORAGE

リソースタイプ： AWS::AppConfig::ConfigurationProfile

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appconfig-hosted-configuration-version-description

AWS AppConfig ホスト設定バージョンに説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： APPCONFIG_HOSTED_CONFIGURATION_VERSION_DESCRIPTION

リソースタイプ： AWS::AppConfig::HostedConfigurationVersion

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appflow-flow-tagged

Amazon AppFlow フローにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPFLOW_FLOW_TAGGED

リソースタイプ： AWS::AppFlow::Flow

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、アフリカ (ケープタウン) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appintegrations-event-integration-description

Amazon AppIntegrations イベント統合に説明があるかどうかを確認します。configuration.Description が存在しない場合、ルールは NON_COMPLIANT です。

識別子： APPINTEGRATIONS_EVENT_INTEGRATION_DESCRIPTION

リソースタイプ： AWS::AppIntegrations::EventIntegration

トリガータイプ: 設定変更

AWS リージョン： アフリカ (ケープタウン) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appintegrations-event-integration-tagged

Amazon AppIntegrations イベント統合にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPINTEGRATIONS_EVENT_INTEGRATION_TAGGED

リソースタイプ： AWS::AppIntegrations::EventIntegration

トリガータイプ: 設定変更

AWS リージョン： アフリカ (ケープタウン) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部

(オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-gateway-route-tagged

AWS App Mesh ゲートウェイルートにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPMESH_GATEWAY_ROUTE_TAGGED

リソースタイプ： AWS::AppMesh::GatewayRoute

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-mesh-deny-tcp-forwarding

AWS App Mesh サービスメッシュのプロキシが、メッシュで定義されているプロキシでデプロイされていないサービスに TCP トラフィックを直接転送しないかどうかを確認します。configuration.Spec.EgressFilter.Type が「ALLOW_ALL」に設定されている場合、ルールは NON_COMPLIANT です。

識別子： APPMESH_MESH_DENY_TCP_FORWARDING

リソースタイプ： AWS::AppMesh::Mesh

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-mesh-tagged

AWS App Mesh メッシュにタグがあるかどうかを確認します。必要に応じて、チェックするルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPMESH_MESH_TAGGED

リソースタイプ： AWS::AppMesh::Mesh

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-route-tagged

AWS App Mesh ルートにタグがあるかどうかを確認します。必要に応じて、チェックするルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPMESH_ROUTE_TAGGED

リソースタイプ： AWS::AppMesh::Route

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボ

ルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-virtual-gateway-backend-defaults-tls

AWS App Mesh 仮想ゲートウェイのバックエンドのデフォルトで、仮想ゲートウェイが TLS を使用してすべてのポートと通信する必要があるかどうかを確認します。configuration.Spec.BackendDefaults.ClientPolicy.Tls.Enforce が false の場合、ルールは NON_COMPLIANT です。

識別子： APPMESH_VIRTUAL_GATEWAY_BACKEND_DEFAULTS_TLS

リソースタイプ： AWS::AppMesh::VirtualGateway

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-virtual-gateway-logging-file-path-exists

AWS App Mesh 仮想ゲートウェイにアクセスログを書き込むファイルパスがあるかどうかを確認します。configuration.Spec.Logging.AccessLog.File.Path が存在しない場合、ルールは NON_COMPLIANT です。

識別子： APPMESH_VIRTUAL_GATEWAY_LOGGING_FILE_PATH_EXISTS

リソースタイプ： AWS::AppMesh::VirtualGateway

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-virtual-gateway-tagged

AWS App Mesh 仮想ゲートウェイにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPMESH_VIRTUAL_GATEWAY_TAGGED

リソースタイプ： AWS::AppMesh::VirtualGateway

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-virtual-node-backend-defaults-tls-on

AWS App Mesh 仮想ノードのバックエンドのデフォルトで、仮想ノードが TLS を使用してすべてのポートと通信する必要があるかどうかを確認します。configuration.Spec.BackendDefaults.ClientPolicy.Tls.Enforce が false の場合、ルールは NON_COMPLIANT です。

識別子： APPMESH_VIRTUAL_NODE_BACKEND_DEFAULTS_TLS_ON

リソースタイプ： AWS::AppMesh::VirtualNode

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシ

フィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-virtual-node-logging-file-path-exists

AWS App Mesh 仮想ノードにアクセスログを書き込むファイルパスがあるかどうかを確認します。configuration.Spec.Logging.AccessLog.File.Path が存在しない場合、ルールは NON_COMPLIANT です。

識別子： APPMESH_VIRTUAL_NODE_LOGGING_FILE_PATH_EXISTS

リソースタイプ： AWS::AppMesh::VirtualNode

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-virtual-node-tagged

AWS App Mesh 仮想ノードにタグがあるかどうかを確認します。必要に応じて、チェックするルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPMESH_VIRTUAL_NODE_TAGGED

リソースタイプ： AWS::AppMesh::VirtualNode

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-virtual-router-tagged

AWS App Mesh 仮想ルーターにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPMESH_VIRTUAL_ROUTER_TAGGED

リソースタイプ： AWS::AppMesh::VirtualRouter

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appmesh-virtual-service-tagged

AWS App Mesh 仮想サービスにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPMESH_VIRTUAL_SERVICE_TAGGED

リソースタイプ： AWS::AppMesh::VirtualService

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

approved-amis-by-id

EC2 インスタンスが指定された Amazon マシンイメージ (AMIsを使用しているかどうかを確認します。承認済み AMI ID のリストを指定します。実行中のインスタンスで使用されている AMI が、このリストにない場合は NON_COMPLIANT です。

識別子: APPROVED_AMIS_BY_ID

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

amiIds, タイプ: CSV

最大 21 の AMI IDs のカンマ区切りリスト。1024 文字の制限があります。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

approved-amis-by-tag

EC2 インスタンスが指定された Amazon マシンイメージ (AMIs) を使用しているかどうかを確認します。AMI を識別するタグを指定します。実行中のインスタンスで使用されている AMI に、指定したタグの少なくとも 1 つがない場合は NON_COMPLIANT です。

識別子:APPROVED_AMIS_BY_TAG

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

amisByTagKeyAndValue, 型: StringMap, デフォルト: tag-key:tag-value,other-tag-key

> 最大 10 個の AMIs タグのカンマ区切りリスト (tag-key:tag-value)。例えば、tag-key1 AMIs を tag-key1 と照合し、tag-key2:value2 は tag-key2 を値 2 と照合します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

apprunner-service-in-vpc

AWS App Runner サービスがカスタム VPC を介して送信トラフィックをルーティングするかどうかを確認します。configuration.NetworkConfiguration.EgressConfiguration.EgressType が DEFAULT と等しい場合、ルールは NON_COMPLIANT です。

識別子： APPRUNNER_SERVICE_IN_VPC

リソースタイプ： AWS::AppRunner::Service

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、欧州 (ロンドン) 、アジ

アパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

apprunner-service-no-public-access

AWS AppRunner サービスがパブリックにアクセス可能でないかどうかを確認します。service.configuration.NetworkConfiguration.IngressConfiguration.IsPubliclyAccessible が False の場合、ルールは NON_COMPLIANT です。

識別子： APPRUNNER_SERVICE_NO_PUBLIC_ACCESS

リソースタイプ： AWS::AppRunner::Service

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

apprunner-service-observability-enabled

AWS App Runner サービスでオブザーバビリティが有効になっているかどうかを確認します。configuration.ObservabilityConfiguration.ObservabilityEnabled が false' の場合、ルールは NON_COMPLIANT です。

識別子： APPRUNNER_SERVICE_OBSERVABILITY_ENABLED

リソースタイプ： AWS::AppRunner::Service

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

apprunner-service-tagged

AWS App Runner サービスにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPRUNNER_SERVICE_TAGGED

リソースタイプ： AWS::AppRunner::Service

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、欧州 (ロンドン) 、アジ

アパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

apprunner-vpc-connector-tagged

AWS App Runner VPC コネクタにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： APPRUNNER_VPC_CONNECTOR_TAGGED

リソースタイプ： AWS::AppRunner::VpcConnector

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appstream-fleet-in-vpc

Amazon AppStream 2.0 フリートが Amazon Virtual Private Cloud (Amazon VPC) を使用しているかどうかを確認します。configuration.VpcConfig が存在しない場合、ルールは NON_COMPLIANT です。ルールは Elastic フリートをチェックしません。

識別子： APPSTREAM_FLEET_IN_VPC

リソースタイプ： AWS::AppStream::Fleet

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appsync-associated-with-waf

AWS AppSync APIs AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられているかどうかを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

識別子: APPSYNC_ASSOCIATED_WITH_WAF

リソースタイプ: AWS::AppSync::GraphQLApi

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

wafWebAclARNs (オプション), タイプ: CSV

認証された Web ACL の Amazon リソースネーム (ARN) のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appsync-authorization-check

AWS AppSync API が許可された認可メカニズムを使用しているかどうかを確認します。承認されていない認可メカニズムが使用されている場合、ルールは NON_COMPLIANT です。

識別子: APPSYNC_AUTHORIZATION_CHECK

リソースタイプ: AWS::AppSync::GraphQLApi

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

AllowedAuthorizationTypes, タイプ: CSV

許可されている AWS AppSync 認可メカニズムをカンマで区切ったリスト。許可される値は、「API_KEY」、「AWS_LAMBDA」、「AWS_IAM」、「OPENID_CONNECT」、「AMAZON_COGNITO_USER_POOLS」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appsync-cache-ct-encryption-at-rest

AWS AppSync API キャッシュで保管時の暗号化が有効になっているかどうかを確認します。'AtRestEncryptionEnabled' が false の場合、このルールは NON_COMPLIANT です。

識別子: APPSYNC_CACHE_CT_ENCRYPTION_AT_REST

リソースタイプ: AWS::AppSync::ApiCache

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appsync-cache-ct-encryption-in-transit

AWS AppSync API キャッシュで転送中の暗号化が有効になっているかどうかを確認します。'TransitEncryptionEnabled' が false の場合、ルールは NON_COMPLIANT です。

識別子: APPSYNC_CACHE_CT_ENCRYPTION_IN_TRANSIT

リソースタイプ: AWS::AppSync::ApiCache

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appsync-cache-encryption-at-rest

AWS AppSync API キャッシュで保管時の暗号化が有効になっているかどうかを確認します。'AtRestEncryptionEnabled' が false の場合、このルールは NON_COMPLIANT です。

識別子: APPSYNC_CACHE_ENCRYPTION_AT_REST

リソースタイプ: AWS::AppSync::GraphQLApi

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

appsync-logging-enabled

AWS AppSync API でログ記録が有効になっているかどうかを確認します。ログ記録が有効になっていない場合、または AWS AppSync API のフィールドログ記録レベルが「」ルールパラメータで指定された値と一致しない場合、`fieldLoggingLevel`ルールは NON_COMPLIANT です。

識別子: APPSYNC_LOGGING_ENABLED

リソースタイプ: AWS::AppSync::GraphQLApi

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

fieldLoggingLevel (オプション), タイプ: CSV

チェックするルールのフィールドログ記録レベルのカンマ区切りリスト。たとえば、「ERROR, INFO」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

athena-data-catalog-description

Amazon Athena データカタログに説明があるかどうかを確認します。configuration.Description が存在しない場合、ルールは NON_COMPLIANT です。

識別子： ATHENA_DATA_CATALOG_DESCRIPTION

リソースタイプ： AWS::Athena::DataCatalog

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

athena-prepared-statement-description

Amazon Athena 準備済みステートメントに説明があるかどうかを確認します。configuration.Description が存在しない場合、ルールは NON_COMPLIANT です。

識別子： ATHENA_PREPARED_STATEMENT_DESCRIPTION

リソースタイプ： AWS::Athena::PreparedStatement

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、欧州 (ミラノ) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

athena-workgroup-description

Amazon Athena ワークグループに説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： ATHENA_WORKGROUP_DESCRIPTION

リソースタイプ: AWS::Athena::WorkGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

athena-workgroup-encrypted-at-rest

Amazon Athena ワークグループが保管中に暗号化されているかどうかを確認します。Athena ワークグループで保管中のデータの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: ATHENA_WORKGROUP_ENCRYPTED_AT_REST

リソースタイプ: AWS::Athena::WorkGroup

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

athena-workgroup-enforce-workgroup-configuration

Athena エンジンを使用する Amazon Athena ワークグループがワークグループ設定を適用してクライアント側の設定を上書きするかどうかを確認します。configuration.WorkGroupConfiguration.EnforceWorkGroupConfiguration が false の場合、ルールは NON_COMPLIANT です。

識別子： ATHENA_WORKGROUP_ENFORCE_WORKGROUP_CONFIGURATION

リソースタイプ: AWS::Athena::WorkGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

athena-workgroup-engine-version-auto-upgrade

Athena エンジンを使用する Amazon Athena ワークグループが自動アップグレードするように設定されているかどうかを確認します。configuration.WorkGroupConfiguration.EngineVersion.SelectedEngineVersion が「AUTO」でない場合、ルールは NON_COMPLIANT です。

識別子： ATHENA_WORKGROUP_ENGINE_VERSION_AUTO_UPGRADE

リソースタイプ: AWS::Athena::WorkGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

athena-workgroup-logging-enabled

Amazon Athena WorkGroup が、使用状況メトリクスを Amazon CloudWatch に公開するかどうかを確認します。Amazon Athena WorkGroup 'PublishCloudWatchMetricsEnabled ' が false に設定されている場合、ルールは NON_COMPLIANT です。

識別子: ATHENA_WORKGROUP_LOGGING_ENABLED

リソースタイプ: AWS::Athena::WorkGroup

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

aurora-last-backup-recovery-point-created

Amazon Aurora DB クラスターのリカバリポイントが作成されたかどうかを確認します。Amazon Relational Database Service (Amazon RDS) DB クラスターに対応するリカバリポイントが指定した期間内に作成されていない場合、ルールは NON_COMPLIANT です。

識別子: AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Aurora DB クラスターのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

ルールの Aurora DB クラスターの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

aurora-meets-restore-time-target

Amazon Aurora DB クラスターの復元時間が、指定された期間と一致しているかどうかを確認します。Aurora DB クラスターの LatestRestoreExecutionTimeMinutes が maxRestoreTime の値より大きい場合、ルールは NON_COMPLIANT です。

識別子: AURORA_MEETS_RESTORE_TIME_TARGET

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各 AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

maxRestoreTime, タイプ: int

最大許容復元ランタイムの数値。

resourceTags (オプション), 型: 文字列

チェックするルールの Aurora DB クラスターのタグ (JSON 形式) 。

resourceId (オプション), 型: 文字列

ルールの Aurora DB クラスターの ID。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

aurora-mysql-backtracking-enabled

Amazon Aurora MySQL クラスターでバックトラッキングが有効になっているかどうかを確認します。Aurora クラスターで MySQL が使用されているが、バックトラッキングが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: AURORA_MYSQL_BACKTRACKING_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、南米 (サンパウロ) 、アジアパシフィック (香港) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、イスラエル (テルアビブ) 、カナダ西部 (カルガリー) 、欧州 (スペイン) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

BacktrackWindowInHours (オプション), 型: 倍精度浮動小数点数

Aurora MySQL クラスターをバックトラックする時間 (時単位) (最大 72 時間)

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

aurora-mysql-cluster-audit-logging

Amazon Aurora MySQL DB クラスターで監査ログ記録が有効になっているかどうかを確認します。DB クラスターで監査ログ記録が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子： AURORA_MYSQL_CLUSTER_AUDIT_LOGGING

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

aurora-resources-in-logically-air-gapped-vault

Amazon Aurora DB クラスターが論理エアギャップボールトにあるかどうかを確認します。Amazon Aurora DB クラスターが、指定された期間内に論理エアギャップボールトにない場合、ルールは NON_COMPLIANT です。

識別子: AURORA_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

resourceTags (オプション), 型: 文字列

チェックするルールの Aurora DB クラスターのタグ (JSON 形式) 。

resourceId (オプション), 型: 文字列

ルールの Aurora DB クラスターの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 2184 以下、日は 91 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

バックアップ計画によって保護された Aurora リソース

Amazon Aurora DB クラスターがバックアッププランで保護されているかどうかを確認します。Amazon Relational Database Service (Amazon RDS) データベースクラスターがバックアッププランによって保護されていない場合、ルールは NON_COMPLIANT です。

識別子:AURORA_RESOURCES_PROTECTED_BACKUP_PLAN

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Aurora DB クラスターのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

ルールの Aurora DB クラスターの ID。

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

autoscaling-capacity-rebalancing

複数のインスタンスタイプを使用する Amazon EC2 Auto Scaling グループで容量の再分散が有効かどうかを確認します。容量の再分散が有効でない場合、ルールは NON_COMPLIANT です。

識別子: AUTOSCALING_CAPACITY_REBALANCING

リソースタイプ: AWS::AutoScaling::AutoScalingGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マ

レーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

autoscaling-group-elb-healthcheck-required

Elastic Load Balancer に関連付けられた Amazon EC2 Auto Scaling グループで、Elastic Load Balancing のヘルスチェックが使用されているかどうかを確認します。Amazon EC2 Auto Scaling グループが Elastic Load Balancing のヘルスチェックを使用していない場合、ルールは NON_COMPLIANT です。

識別子: AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

リソースタイプ: AWS::AutoScaling::AutoScalingGroup

トリガータイプ: 設定変更

AWS リージョン： 中東 (アラブ首長国連邦) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、[AWS Config 「ルールを使用したリソースの評価](#)」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すに

は、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

*有効な値は EC2 (デフォルト)、ELB、VPC_LATTICE です。VPC_LATTICE ヘルスチェックタイプはプレビューリリースの VPC Lattice 用に予約されており、変更される可能性があります。詳細については、Amazon EC2 Auto Scaling ユーザーガイドの「Auto Scaling インスタンスのヘルスチェック」を参照してください。

プロアクティブ評価の詳細については、「Evaluation Mode」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

autoscaling-launchconfig-requires-imdsv2

IMDSv2 だけが有効になっているかどうかを確認します。メタデータのバージョンが起動設定に含まれていない場合、またはメタデータ V1 と V2 の両方が有効になっている場合、このルールは非準拠です。

識別子: AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2

リソースタイプ: AWS::AutoScaling::LaunchConfiguration

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

autoscaling-launch-config-hop-limit

メタデータトークンが移動できるネットワークホップの数を確認します。メタデータのレスポンスのホップ制限が 1 より大きい場合、このルールは NON_COMPLIANT です。

識別子: AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

リソースタイプ: AWS::AutoScaling::LaunchConfiguration

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

autoscaling-launch-config-public-ip-disabled

Amazon EC2 Auto Scaling グループのパブリック IP アドレスが、起動設定によって有効になっているかどうかを確認します。Amazon EC2 Auto Scaling グループの起動設定

で、AssociatePublicIpAddress が「true」に設定されている場合、このルールは NON_COMPLIANT です。

識別子: AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

リソースタイプ: AWS::AutoScaling::LaunchConfiguration

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

autoscaling-launch-template

対象の Amazon Elastic Compute Cloud (EC2) Auto Scaling グループが、EC2 起動テンプレートから作成されたものかどうかを確認します。EC2 起動テンプレートから作成されていない Scaling グループでは、ルールが NON_COMPLIANT になっています。

識別子: AUTOSCALING_LAUNCH_TEMPLATE

リソースタイプ: AWS::AutoScaling::AutoScalingGroup

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

autoscaling-multiple-az

Auto Scaling グループが複数のアベイラビリティーゾーンにまたがっているかどうかを確認します。Auto Scaling グループが複数のアベイラビリティーゾーンにまたがっていない場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): AUTOSCALING_MULTIPLE_AZ

リソースタイプ: AWS::AutoScaling::AutoScalingGroup

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

minAvailabilityZones (オプション), タイプ: int

期待されるアベイラビリティーゾーンの最小数です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

autoscaling-multiple-instance-types

Amazon EC2 Auto Scaling グループが複数のインスタンスタイプを使用しているかどうかを確認します。Amazon EC2 Auto Scaling グループにインスタンスタイプが 1 つしか定義されていない場

合、ルールは NON_COMPLIANT です。このルールは、属性ベースのインスタンスタイプを評価しません。

識別子: AUTOSCALING_MULTIPLE_INSTANCE_TYPES

リソースタイプ: AWS::AutoScaling::AutoScalingGroup

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

バックアップ計画-分-頻度と分保持チェック

バックアッププランに、必要な頻度と保存期間を満たすバックアップルールがあるかどうかを確認します。このルールは、少なくとも指定した頻度と同じ頻度でリカバリポイントが作成されない場合、または指定した期間より前に期限切れになる場合は、非準拠です。

識別子:BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

リソースタイプ: AWS::Backup::BackupPlan

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

必須周波数値 (オプション), タイプ: int, デフォルト: 1

必要なバックアップ頻度の数値 最大 24 時間、31 日間。

必要な保持日数 (オプション), タイプ: int, デフォルト: 35

必要な保存期間 (日単位)

必須周波数単位 (オプション), 型: 文字列, デフォルト:日単位

必要なバックアップ頻度の単位時間です。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

バックアップ/リカバリポイント暗号化

リカバリポイントが暗号化されているかどうかを確認します。リカバリポイントが暗号化されていない場合、ルールは NON_COMPLIANT です。

識別子:BACKUP_RECOVERY_POINT_ENCRYPTED

リソースタイプ: AWS::Backup::RecoveryPoint

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

バックアップ/リカバリポイントの手動削除/無効化

バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されているかどうかを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolic アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

> **Note**
>
> Deny ステートメント**"Principal"**の **"Resource"**および に必要なワイルドカード
> このルールでは、拒否ステートメント"Principal"の "Resource"および にボールトアクセスポリシーにワイルドカードが必要です。それ以外の場合、ルールは NON_COMPLIANT を返します。

識別子:BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

リソースタイプ: AWS::Backup::BackupVault

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

PrincipalArnList (オプション), タイプ: CSV

> チェックしないルールの AWS Identity and Access Management (IAM) Amazon リソースネーム (ARNsのカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

バックアップ/リカバリポイントの最小保存期間チェック

リカバリポイントが、指定した期間より前に期限切れになるかどうかを確認します。リカバリポイントに必要な保持期間より短いリテンションポイントがある場合、ルールは NON_COMPLIANT です。

識別子:BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

リソースタイプ: AWS::Backup::RecoveryPoint

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

必要な保持日数 (オプション), タイプ: int, デフォルト: 35

必要な保存期間 (日単位)

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

batch-compute-environment-enabled

AWS バッチコンピューティング環境が有効になっているかどうかを確認します。configuration.State が「DISABLED」の場合、ルールは NON_COMPLIANT です。

識別子： BATCH_COMPUTE_ENVIRONMENT_ENABLED

リソースタイプ： AWS::Batch::ComputeEnvironment

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

batch-compute-environment-managed

AWS バッチコンピューティング環境が管理されているかどうかを確認します。configuration.Type が「UNMANAGED」の場合、ルールは NON_COMPLIANT です。

識別子： BATCH_COMPUTE_ENVIRONMENT_MANAGED

リソースタイプ： AWS::Batch::ComputeEnvironment

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

batch-compute-environment-tagged

AWS バッチコンピューティング環境にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： BATCH_COMPUTE_ENVIRONMENT_TAGGED

リソースタイプ： AWS::Batch::ComputeEnvironment

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

batch-job-queue-enabled

AWS バッチジョブキューが有効になっているかどうかを確認します。configuration.State が「DISABLED」の場合、ルールは NON_COMPLIANT です。

識別子： BATCH_JOB_QUEUE_ENABLED

リソースタイプ： AWS::Batch::JobQueue

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

batch-job-queue-tagged

AWS バッチジョブキューにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： BATCH_JOB_QUEUE_TAGGED

リソースタイプ： AWS::Batch::JobQueue

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

batch-managed-compute-environment-using-launch-template

AWS バッチマネージドコンピューティング環境が起動テンプレートを使用して設定されているかどうかを確認します。configuration.ComputeResources.LaunchTemplate が存在しない場合、ルールは NON_COMPLIANT です。

識別子： BATCH_MANAGED_COMPUTE_ENVIRONMENT_USING_LAUNCH_TEMPLATE

リソースタイプ： AWS::Batch::ComputeEnvironment

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

batch-managed-compute-env-compute-resources-tagged

AWS バッチマネージドコンピューティング環境のコンピューティングリソースにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。「aws:」で始まるタグはチェックされません。

識別子： BATCH_MANAGED_COMPUTE_ENV_COMPUTE_RESOURCES_TAGGED

リソースタイプ： AWS::Batch::ComputeEnvironment

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西

部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

batch-scheduling-policy-tagged

AWS バッチスケジューリングポリシーにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： BATCH_SCHEDULING_POLICY_TAGGED

リソースタイプ： AWS::Batch::SchedulingPolicy

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

beanstalk-enhanced-health-reporting-enabled

Elastic Beanstalk AWS 環境が拡張ヘルスレポート用に設定されているかどうかを確認します。この環境が拡張ヘルスレポートを作成するよう設定されている場合、ルールは COMPLIANT です。環境が基本ヘルスレポートを作成するよう設定されている場合、ルールは NON_COMPLIANT です。

識別子: BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

リソースタイプ: AWS::ElasticBeanstalk::Environment

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cassandra-keyspace-tagged

Amazon Keyspaces (Apache Cassandra 用) キースペースにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： CASSANDRA_KEYSPACE_TAGGED

リソースタイプ： AWS::Cassandra::Keyspace

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、中東 (バーレーン) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、アジアパシフィック (香港) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

clb-desync-mode-check

Classic Load Balancer (CLB) がユーザー定義の Desync 軽減モードで設定されているかどうかを確認します。CLB Desync 軽減モードがユーザー定義の Desync 軽減モードと一致しない場合、ルールは NON_COMPLIANT です。

識別子: CLB_DESYNC_MODE_CHECK

リソースタイプ: AWS::ElasticLoadBalancing::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガ

リー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

desyncMode, タイプ: CSV

値のカンマ区切りリスト。最大 2 つを選択できます。有効な値は、「Defensive」、「Strictest」、「Monitor」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

clb-multiple-az

Classic Load Balancer が複数のアベイラビリティーゾーン (AZ) にまたがるかどうかをチェックします。Classic Load Balancer が 2 AZ 未満の場合、または `minAvailabilityZones` パラメータ (指定されている場合) に記載されている数の AZ にまたがっていない場合は、ルールは NON_COMPLIANT です。

識別子: CLB_MULTIPLE_AZ

リソースタイプ: AWS::ElasticLoadBalancing::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

minAvailabilityZones (オプション), タイプ: int

期待される AZ の必要な最小数。有効な値は、2 ~ 10 で、両方とも含まれます。パラメータが指定されていない場合、デフォルトは 2 です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudformation-stack-drift-detection-check

a AWS CloudFormation （ AWS CloudFormation) スタックの実際の設定が、予想される設定と異なるか、ドリフトしたかどうかを確認します。スタックの 1 つ以上のリソースが意図した設定と異なっている場合、スタックはドリフトしたと見なされます。このルールとスタックは、スタックのドリフトステータスが IN_SYNC の場合、COMPLIANT です。このルールは、スタックのドリフトステータスが DRIFTED の場合、NON_COMPLIANT です。

> **Note**
>
> このルールでは、アカウント内の各スタックで DetectStackDrift オペレーションを実行します。スタックに含まれるリソースの数によっては、DetectStackDrift オペレーションに数分かかることがあります。このルールの最大実行時間は 15 分に制限されているため、アカウント内のすべてのスタックの評価が完了する前にルールがタイムアウトする可能性があります。
> この問題が発生した場合は、タグを使用してルールの対象となるスタック数を制限することを推奨します。以下の操作を行うことができます。
>
> 1. スタックをグループに分け、それぞれに異なるタグを付けます。
> 2. そのグループのすべてのスタックに、同じタグを適用します。
> 3. アカウントにはこのルールのインスタンスを複数用意し、それぞれを異なるタグでスコープを指定します。これにより、ルールの各インスタンスは、対応するタグがスコープに記述されているスタックのみを処理できます。

識別子: CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

リソースタイプ: AWS::CloudFormation::Stack

トリガータイプ: 設定変更および定期的

AWS リージョン： アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (メルボルン) 、イスラエル (テルアビブ) 、カナ

ダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

cloudformationRoleArn, タイプ: 文字列

AWS CloudFormation スタックのドリフトを検出するポリシーアクセス許可を持つ IAM ロールの Amazon リソースネーム (ARN)。ロールに必要な IAM 権限については、 ユーザーガイドの「スタックとリソースに対するアンマネージド型構成変更の検出 | ドリフトを検出する際の考慮事項」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

cloudformation-stack-notification-check

CloudFormation スタックが Amazon SNS トピックにイベント通知を送信しているかどうか確認します。オプションで、指定された Amazon SNS トピックが使用されているかどうか確認します。CloudFormation スタックが通知を送信しない場合、ルールは NON_COMPLIANT です。

識別子: CLOUDFORMATION_STACK_NOTIFICATION_CHEC

リソースタイプ: AWS::CloudFormation::Stack

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

snsTopic1 (オプション), 型: 文字列

SNS トピック ARN。

snsTopic2 (オプション), 型: 文字列

SNS トピック ARN。

snsTopic3 (オプション), 型: 文字列

SNS トピック ARN。

snsTopic4 (オプション), 型: 文字列

SNS トピック ARN。

snsTopic5 (オプション), 型: 文字列

SNS トピック ARN。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-accesslogs-enabled

Amazon CloudFront ディストリビューションが、標準ログ記録 (レガシー) を使用して Amazon S3 バケットにアクセスログを配信するように設定されているかどうかを確認します。CloudFront ディストリビューションにレガシーログ記録が設定されていない場合、ルールは NON_COMPLIANT です。

識別子: CLOUDFRONT_ACCESSLOGS_ENABLED

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

S3BucketName (オプション), 型: 文字列

サーバーアクセスログを保存するための Amazon S3 バケットの名前。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-associated-with-waf

Amazon CloudFront ディストリビューションがウェブアプリケーションファイアウォール (WAF) または WAFv2 ウェブアクセスコントロールリスト (ACL) に関連付けられているかどうかを確認します。CloudFront ディストリビューションが WAF ウェブ ACL に関連付けられていない場合、ルールは NON_COMPLIANT です。

識別子: CLOUDFRONT_ASSOCIATED_WITH_WAF

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

wafWebAclIds (オプション), タイプ: CSV

> WAF のウェブ ACL ID のカンマ区切りリスト、または WAFV2 のウェブ ACL Amazon リソースネーム (ARN)。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-custom-ssl-certificate

Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの Secure Sockets Layer (SSL) 証明書であるかどうかを確認します。

識別子: CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-default-root-object-configured

Amazon CloudFront ディストリビューションが、デフォルトのルートオブジェクトである特定のオブジェクトを返すように設定されているかどうかを確認します。

識別子: CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-no-deprecated-ssl-protocols

CloudFront ディストリビューションが CloudFront エッジロケーションとカスタムオリジン間の HTTPS 通信に非推奨の SSL プロトコルを使用しているかどうかを確認します。

「OriginSslProtocols」に「SSLv3」が含まれる場合、このルールは CloudFront ディストリビューションでは非準拠です。

識別子: CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-origin-access-identity-enabled

Amazon S3 オリジンタイプの CloudFront ディストリビューションにオリジンアクセスアイデンティティが設定されているかどうかを確認します。CloudFront ディストリビューションが S3 によってバックアップされていて、オリジンタイプが OAI に設定されていない場合、またはオリジンが S3 バケットでない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> オリジンが S3 バケットで`NOT_APPLICABLE`ない場合、ルールは を返しません。

識別子: CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-origin-failover-enabled

Amazon CloudFront ディストリビューションがオリジングループに少なくとも 2 つのオリジンで構成されているかどうかを確認します。

識別子: CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-s3-origin-access-control-enabled

Amazon Simple Storage Service (Amazon S3) オリジンタイプを使用する Amazon CloudFront ディストリビューションで、オリジンアクセスコントロール (OAC) が有効かどうかをチェックします。OAC が有効になっていない Amazon S3 オリジンを使用する CloudFront ディストリビューションの場合、ルールは NON_COMPLIANT になります。

識別子: CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-s3-origin-non-existent-bucket

Amazon CloudFront ディストリビューションが、存在しない S3 バケットを指しているかどうかを確認します。CloudFront ディストリビューションの `S3OriginConfig` が存在しない S3 バケットを指している場合、ルールは NON_COMPLIANT となります。このルールでは、静的ウェブサイトホスティングの S3 バケットは評価されません。

識別子: CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 定期的

AWS リージョン: 中国 (北京)、米国東部 (バージニア北部) リージョンでのみ利用できます

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-security-policy-check

Amazon CloudFront ディストリビューションが、ビューワー接続に必要な最低限のセキュリティポリシーと、TLSv1.2 以上の暗号スイートを使用しているかどうかを確認します。minimumProtocolVersion が TLSv1.2_2018 より古い場合、CloudFront ディストリビューションでは、このルールは NON_COMPLIANT です。

識別子: CLOUDFRONT_SECURITY_POLICY_CHECK

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-sni-enabled

このルールは、CloudFront ディストリビューションが SNI を使用して HTTPS リクエストを処理するように設定されているかどうかを確認します。

識別子: CLOUDFRONT_SNI_ENABLED

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-ssl-policy-check

Amazon CloudFront ディストリビューションが指定されたセキュリティポリシーで設定されているかどうかを確認します。CloudFront ディストリビューションが指定されたセキュリティポリシーで設定されていない場合、ルールは NON_COMPLIANT です。

識別子： CLOUDFRONT_SSL_POLICY_CHECK

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

パラメータ：

securityPolicies, タイプ: CSV

> チェックするルールの CloudFront ディストリビューションセキュリティポリシーのカンマ区切りリスト。例: "TLSv1.2_2018, TLSv1.2_2019, TLSv1.2_2021". 有効な値のリストについては、Amazon CloudFront デベロッパーガイド」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-traffic-to-origin-encrypted

Amazon CloudFront ディストリビューションがカスタムオリジンへのトラフィックを暗号化しているかどうかを確認します。「OriginProtocolPolicy」が「http のみ」の場合、または「OriginProtocolPolicy」が「マッチビューア」で「ViewerProtocolPolicy」が「すべて許可」の場合、ルールは非準拠です。

識別子: CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudfront-viewer-policy-https

Amazon CloudFront ディストリビューションが HTTPS を (直接またはリダイレクト経由で) 使用しているかどうかを確認します。ViewerProtocolPolicy の値が DefaultCacheBehavior または CacheBehaviors に対して「allow-all」に設定されている場合、ルールは NON_COMPLIANT です。

Identifier: CLOUDFRONT_VIEWER_POLICY_HTTPS

リソースタイプ: AWS::CloudFront::Distribution

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudtrail-all-read-s3-data-event-check

AWS CloudTrail マルチリージョン証跡が有効になっているかどうかを確認し、バケットのすべての読み取り S3 データイベントをログに記録します。マルチリージョン証跡が現在および将来のすべての S3 バケットのすべての読み取り S3 データイベントタイプを記録しない場合、ルールは NON_COMPLIANT です。

識別子: CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudtrail-all-write-s3-data-event-check

AWS CloudTrail マルチリージョン証跡が有効になっているかどうかを確認し、バケットのすべての書き込み S3 データイベントをログに記録します。マルチリージョン証跡が現在および将来のすべての S3 バケットのすべての書き込み S3 データイベントタイプをログに記録しない場合、ルールは NON_COMPLIANT です。

識別子: CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudtrail-s3-bucket-access-logging

AWS CloudTrail ログの S3 バケット設定で Amazon S3 サーバーアクセスログが有効になっているかどうかを確認します。CloudTrail 証跡の少なくとも 1 つの S3 バケットで S3 サーバーアクセスログ記録が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

リソースタイプ: AWS::CloudTrail::Trail

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudtrail-s3-bucket-public-access-prohibited

AWS CloudTrail ログの S3 バケット設定がパブリックアクセスをブロックしているかどうかを確認します。CloudTrail 証跡の少なくとも 1 つの S3 バケットに対してパブリックアクセスがある場合、ルールは NON_COMPLIANT です。

識別子: CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROHIBITED

リソースタイプ: AWS::CloudTrail::Trail

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudtrail-s3-dataevents-enabled

少なくとも 1 つの AWS CloudTrail 証跡がすべての Amazon S3S3) データイベントをログに記録しているかどうかを確認します。証跡がある場合、または証跡が S3 データイベントを記録していない場合、ルールは NON_COMPLIANT です。

識別子: CLOUDTRAIL_S3_DATAEVENTS_ENABLED

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

S3BucketNames (オプション), 型: 文字列

データイベントのログ記録を有効にする S3 バケット名のカンマ区切りリスト。デフォルトでは、すべての S3 バケットをチェックします。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudtrail-security-trail-enabled

セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:

- グローバルサービスイベントを記録すること
- マルチリージョンの証跡であること
- ログファイル検証が有効になっていること
- KMS キーで暗号化されていること
- 読み取りと書き込みのイベントを記録すること
- 管理イベントを記録すること
- 管理イベントを除外しないこと

上記の基準をすべて満たす証跡がない場合、このルールは NON_COMPLIANT です。

識別子: CLOUDTRAIL_SECURITY_TRAIL_ENABLED

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudwatch-alarm-action-check

CloudWatch のアラームに ALARM、INFUFICIENT_DATA、または OK の状態に設定されたアクションがあるかどうかを確認します。オプションで、指定した ARN に一致するアクションがあるかどうかを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

識別子: CLOUDWATCH_ALARM_ACTION_CHECK

リソースタイプ: AWS::CloudWatch::Alarm

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

alarmActionRequired, 型: 文字列, デフォルト: true

アラームには少なくとも 1 つのアクションがあります。

insufficientDataActionRequired, 型: 文字列, デフォルト: true

アラームが別の状態から INSUFFICIENT_DATA の状態に移行する場合、アラームには少なくとも 1 つのアクションがあります。

okActionRequired, 型: 文字列, デフォルト: false

アラームが別の状態から OK の状態に移行する場合、アラームには少なくとも 1 つのアクションがあります。

action1 (オプション), 型: 文字列

実行するアクション (ARN として指定)。

action2 (オプション), 型: 文字列

実行するアクション (ARN として指定)。

action3 (オプション), 型: 文字列

実行するアクション (ARN として指定)。

action4 (オプション), 型: 文字列

実行するアクション (ARN として指定)。

action5 (オプション), 型: 文字列

実行するアクション (ARN として指定)。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudwatch-alarm-action-enabled-check

Amazon CloudWatch アラームアクションが有効な状態にあるかどうかをチェックします。CloudWatch アラームアクションが有効状態でない場合、ルールは NON_COMPLIANT です。

識別子: CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

リソースタイプ: AWS::CloudWatch::Alarm

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudwatch-alarm-resource-check

リソースタイプに、名前付きメトリクスの CloudWatch アラームがあるかどうかを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。

識別子: CLOUDWATCH_ALARM_RESOURCE_CHECK

リソースタイプ: AWS::EC2::Instance、AWS::RDS::DBCluster、AWS::S3::Bucket, AWS::EC2::Volume

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

resourceType, タイプ: 文字列

AWS リソースタイプ。値には、AWS::EC2::Volume、AWS::EC2::Instance、AWS::RDS::DBCluster または、AWS:: S3:: Busket のいずれかを指定できます。

metricName, 型: 文字列

アラームに関連付けられているメトリクスの名前 (例: EC2 インスタンスの 'CPUUtilization')。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudwatch-alarm-settings-check

特定のメトリクス名を持つ CloudWatch アラームに指定された設定があるかどうかを確認します。

識別子: CLOUDWATCH_ALARM_SETTINGS_CHECK

リソースタイプ: AWS::CloudWatch::Alarm

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

metricName, 型: 文字列

アラームに関連付けられているメトリクスの名前。

threshold (オプション), タイプ: int

指定した Statistic の値と比較する値。

evaluationPeriods (オプション), タイプ: int

指定した Threshold の値とデータを比較する時間。

period (オプション), タイプ: int, デフォルト: 300

指定した統計の値を適用する時間 (秒)。

comparisonOperator (オプション), 型: 文字列

指定した統計としきい値の比較演算 (例: 'GreaterThanThreshold')。

statistic (オプション), 型: 文字列

アラームに関連付けられているメトリクスの統計 (例: 'Average' または 'Sum')。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudwatch-log-group-encrypted

Amazon CloudWatch Log Groups が KMS AWS キーまたは指定された KMS AWS キー ID で暗号化されているかどうかを確認します。CloudWatch ロググループが KMS キーで暗号化されていない場合、またはルールパラメータに指定されていない KMS キーで暗号化されている場合、ルールは NON_COMPLIANT になります。

識別子: CLOUDWATCH_LOG_GROUP_ENCRYPTED

リソースタイプ: AWS::Logs::LogGroup

トリガータイプ: 定期的

AWS リージョン： 中東 (アラブ首長国連邦) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

KmsKeyId (オプション), タイプ: 文字列

ロググループの暗号化に使用される KMS キーの ID の Amazon リソースネーム (ARN)。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloud-trail-cloud-watch-logs-enabled

AWS CloudTrail 証跡が CloudWatch Logs にログを送信するように設定されているかどうかを確認します。証跡の CloudWatchLogsLogGroupArn プロパティが空の場合、この証跡は NON_COMPLIANT です。

識別子: CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

リソースタイプ: AWS::CloudTrail::Trail

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

expectedDeliveryWindowAge (オプション), タイプ: int

コンプライアンスを満たす CloudWatch Logs への最新の配信の最大経過時間 (時単位)

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloudtrail-enabled

> **Important**
>
> このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。

AWS アカウントで AWS CloudTrail 証跡が有効になっているかどうかを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

識別子: CLOUD_TRAIL_ENABLED

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

s3BucketNames (オプション), 型: 文字列

CloudTrail ログファイルの配信先 S3 バケットの名前。

snsTopicArn (オプション), 型: 文字列

CloudTrail 通知に使用される SNS トピック ARN。

cloudWatchLogsLogGroupArn (オプション), 型: 文字列

CloudTrail のデータ送信先となる CloudWatch ロググループ ARN。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloud-trail-encryption-enabled

サーバー側の暗号化 (SSE) AWS Key Management Service（AWS KMS) 暗号化を使用するように AWS CloudTrail が設定されているかどうかを確認します。KmsKeyId が定義されている場合、ルールは COMPLIANT です。

識別子: CLOUD_TRAIL_ENCRYPTION_ENABLED

リソースタイプ: AWS::CloudTrail::Trail

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cloud-trail-log-file-validation-enabled

AWS CloudTrail が logs. AWS recommends を含む署名付きダイジェストファイルを作成するかどうかを確認します。すべての証跡でファイル検証を有効にすることをお勧めします。検証が有効化されていない場合は、ルールは NON_COMPLIANT です。

識別子: CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

リソースタイプ: AWS::CloudTrail::Trail

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cmk-backing-key-rotation-enabled

キーごとに自動キーローテーションが有効になっているかどうかをチェックし、お客様が作成した KMS キーのキー ID AWS と一致します。リソースの Config AWS レコーダーロールに kms:DescribeKey アクセス許可がない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> 自動キーローテーションは、非対称 KMS キー、HMAC KMS キー、インポートされたキーマテリアルを持つ KMS キー、またはカスタムキーストア内の KMS キーではサポートされていません。

識別子: CMK_BACKING_KEY_ROTATION_ENABLED

リソースタイプ: AWS::KMS::Key

トリガータイプ: 定期的

AWS リージョン： 中東 (アラブ首長国連邦) AWS リージョンを除く、サポートされているすべてのリージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codebuild-project-artifact-encryption

AWS CodeBuild プロジェクトで、すべてのアーティファクトに対して暗号化が有効になっているかどうかを確認します。プライマリまたはセカンダリ (存在する場合) のアーティファクト設定のいずれかに「encryptionDisabled」が「true」に設定されていると、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

リソースタイプ: AWS::CodeBuild::Project

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codebuild-project-environment-privileged-check

AWS CodeBuild プロジェクト環境で特権モードが有効になっているかどうかを確認します。「privilegedMode」が「true」に設定されている場合、ルールは CodeBuild プロジェクトに対して NON_COMPLIANT になります。

[Identifier] (識別子): CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

リソースタイプ: AWS::CodeBuild::Project

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

exemptedProjects (オプション), タイプ: CSV

値が「true」の「privilegedMode」を持つことが許可されている CodeBuild プロジェクトの名前のコンマ区切りのリストです。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codebuild-project-envvar-awscred-check

プロジェクトに環境 variables AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が含まれているかどうかを確認します。プロジェクト環境変数にプレーンテキストの認証情報が含まれている場合、ルールは NON_COMPLIANT です。

識別子: CODEBUILD_PROJECT_ENVVAR_AWSCRED_CHECK

リソースタイプ: AWS::CodeBuild::Project

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codebuild-project-logging-enabled

AWS CodeBuild プロジェクト環境で少なくとも 1 つのログオプションが有効になっているかどうかを確認します。存在するすべてのログ設定のステータスが「DISABLED」に設定されている場合、ルールは NON_COMPLIANT です。

[Identifier] (識別子): CODEBUILD_PROJECT_LOGGING_ENABLED

リソースタイプ: AWS::CodeBuild::Project

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

s3BucketNames (オプション), 型: 文字列

Amazon S3 ログが設定されている場合にログを送信する必要がある S3 バケットの名前のカンマ区切りのリストです。

cloudWatchGroupNames (オプション), 型: 文字列

Amazon CloudWatch ログが設定されている場合にログを送信する必要がある CloudWatch ロググループの名前のカンマ区切りのリストです。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codebuild-project-s3-logs-encrypted

Amazon S3 Logs で設定された AWS CodeBuild プロジェクトで、ログに対して暗号化が有効になっているかどうかを確認します。CodeBuild プロジェクトの s3LogsConfig で「encryptionDisabled」が「true」に設定されている場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

リソースタイプ: AWS::CodeBuild::Project

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

exemptedProjects (オプション), タイプ: CSV

> 暗号化されていないログの出力が許可されている CodeBuild プロジェクトの名前のコンマ区切りのリストです。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codebuild-project-source-repo-url-check

Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれているかどうかを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。

識別子: CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

リソースタイプ: AWS::CodeBuild::Project

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codebuild-report-group-encrypted-at-rest

AWS CodeBuild レポートグループで保管時の暗号化設定が有効になっているかどうかを確認します。EncryptionDisabled」が「true」の場合、ルールは NON_COMPLIANT です。

識別子: CODEBUILD_REPORT_GROUP_ENCRYPTED_AT_REST

リソースタイプ: AWS::CodeBuild::ReportGroup

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codedeploy-auto-rollback-monitor-enabled

デプロイグループに、アラームがアタッチされた自動デプロイロールバックとデプロイモニタリングが設定されているかどうかを確認します。AutoRollbackConfiguration もしくは AlarmConfiguration が設定されていない、または有効化されていない場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

リソースタイプ: AWS::CodeDeploy::DeploymentGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codedeploy-deployment-group-auto-rollback-enabled

AWS CodeDeploy デプロイグループで自動ロールバック設定が有効になっているかどうかを確認します。configuration.autoRollbackConfiguration.enabled が false であるか、存在しない場合、ルールは NON_COMPLIANT です。

識別子： CODEDEPLOY_DEPLOYMENT_GROUP_AUTO_ROLLBACK_ENABLED

リソースタイプ: AWS::CodeDeploy::DeploymentGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codedeploy-deployment-group-outdated-instances-update

AWS CodeDeploy デプロイグループが古いインスタンスを自動的に更新するかどうかをチェックします。configuration.outdatedInstancesStrategy が「IGNORE」の場合、ルールは NON_COMPLIANT です。

識別子： CODEDEPLOY_DEPLOYMENT_GROUP_OUTDATED_INSTANCES_UPDATE

リソースタイプ: AWS::CodeDeploy::DeploymentGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codedeploy-ec2-minimum-healthy-hosts-configured

EC2/オンプレミスコンピューティングプラットフォームのデプロイグループに、正常なホストフリートの最小割合、または入力しきい値以上のホスト数が設定されているかどうかを確認します。どちらかがしきい値を下回っている場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED

リソースタイプ: AWS::CodeDeploy::DeploymentGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

minimumHealthyHostsFleetPercent (オプション), タイプ: int, デフォルト: 66

デプロイ中における正常なホストフリートの最小割合です。デフォルト値は 66% です。

minimumHealthyHostsHostCount (オプション), タイプ: int, デフォルト: 1

デプロイ中におけるフリート内の正常なホストの最小数です。デフォルト値は、1 に設定されています。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codedeploy-lambda-allatonce-traffic-shift-disabled

Lambda コンピューティングプラットフォームのデプロイグループがデフォルトのデプロイ設定を使用していないかどうかを確認します。デプロイグループが「CodeDeployDefault.LambdaAllAtOnce」のデプロイ設定を使用している場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

リソースタイプ: AWS::CodeDeploy::DeploymentGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codeguruprofiler-profiling-group-tagged

Amazon CodeGuru Profiler プロファイリンググループにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： CODEGURUPROFILER_PROFILING_GROUP_TAGGED

リソースタイプ： AWS::CodeGuruProfiler::ProfilingGroup

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codegururevieweer-repository-association-tagged

Amazon CodeGuru Reviewer リポジトリの関連付けにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： CODEGURUREVIEWER_REPOSITORY_ASSOCIATION_TAGGED

リソースタイプ： AWS::CodeGuruReviewer::RepositoryAssociation

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codepipeline-deployment-count-check

AWS CodePipeline の最初のデプロイステージが複数のデプロイを実行するかどうかを確認します。必要に応じて、後続の残りの各ステージで、指定された数 (`deploymentLimit`) を超えるデプロイが実行されているかどうかを確認します。

識別子: CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

リソースタイプ: AWS::CodePipeline::Pipeline

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

deploymentLimit (オプション), タイプ: int

各ステージで実行できるデプロイメントの最大数。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

codepipeline-region-fanout-check

AWS CodePipeline の各ステージが、 AWS CodePipeline が前のすべての結合ステージにデプロイしたリージョンの数の N 倍以上にデプロイされるかどうかを確認します。N はリージョンファンアウト番号です。最初のデプロイステージでは最大 1 個のリージョンにデプロイでき、2 番目のデプロイステージでは `regionFanoutFactor` で指定された最大数までデプロイできます。`regionFanoutFactor` を指定しない場合、デフォルト値は 3 です。例えば、最初のデプロイステージで 1 つのリージョンにデプロイし、2 番目のデプロイステージで 3 つのリージョンにデプロイする場合、3 番目のデプロイステージでは 12 のリージョン、つまり、以前のステージの合計数にファンアウトリージョン数 (3) を乗算した数までデプロイできます。ルールは、デプロイ先の数が第 1 ステージで 1 リージョン、2 番目のステージで 3 リージョン、または 3 番目のステージで 12 リージョンを超える場合、ルールは NON_COMPLIANT です。

識別子: CODEPIPELINE_REGION_FANOUT_CHECK

リソースタイプ: AWS::CodePipeline::Pipeline

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、中東 (アラブ首長国連邦) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、アジアパシフィック (ハイデラバード) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、イスラエル (テルアビブ) 、カナダ (中部) リージョンでのみ利用可能です。

パラメータ :

regionFanoutFactor (オプション), タイプ: int, デフォルト: 3

> AWS CodePipeline が以前のすべてのステージでデプロイしたリージョンの数は、ステージがデプロイできるリージョンの許容数です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cognito-identity-pool-unauth-access-check

Amazon Cognito ID プールで認証されていない ID が許可されているかどうかを確認します。ID プールが認証されていない ID を許可するように設定されている場合、ルールは NON_COMPLIANT です。

識別子： COGNITO_IDENTITY_POOL_UNAUTH_ACCESS_CHECK

リソースタイプ： AWS::Cognito::IdentityPool

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (ソウル) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cognito-user-pool-advanced-security-enabled

Amazon Cognito ユーザープールで、標準認証に対して高度なセキュリティが有効になっているかどうかを確認します。高度なセキュリティが有効になっていない場合、ルールは NON_COMPLIANT です。必要に応じて、ルールがチェックするアドバンストセキュリティモードを指定できます。

識別子: COGNITO_USER_POOL_ADVANCED_SECURITY_ENABLED

リソースタイプ: AWS::Cognito::UserPool

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (香港) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

SecurityMode (オプション) , タイプ: 文字列

> チェックするルールのアドバンストセキュリティモードの文字列値。指定した場合、ユーザープールのアドバンストセキュリティモードがこのパラメータ値と一致しない場合、ルールは NON_COMPLIANT です。有効な値は AUDIT と ENFORCED です

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cognito-user-pool-tagged

Amazon Cognito ユーザープールにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： COGNITO_USER_POOL_TAGGED

リソースタイプ: AWS::Cognito::UserPool

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

connect-instance-logging-enabled

Amazon Connect インスタンスで Amazon CloudWatch ロググループでフローログが有効になっているかどうかを確認します。Amazon Connect インスタンスでフローログが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子： CONNECT_INSTANCE_LOGGING_ENABLED

リソースタイプ： AWS::Connect::Instance

トリガータイプ: 設定変更

AWS リージョン： アフリカ (ケープタウン) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

customerprofiles-object-type-allow-profile-creation

Amazon Connect Customer Profiles オブジェクトタイプで、新しい標準プロファイルが存在しない場合に作成できるかどうかを確認します。configuration.AllowProfileCreation が false の場合、ルールは NON_COMPLIANT です。

識別子： CUSTOMERPROFILES_OBJECT_TYPE_ALLOW_PROFILE_CREATION

リソースタイプ： AWS::CustomerProfiles::ObjectType

トリガータイプ: 設定変更

AWS リージョン： アフリカ (ケープタウン) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

customerprofiles-object-type-tagged

Amazon Connect Customer Profiles オブジェクトタイプにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： CUSTOMERPROFILES_OBJECT_TYPE_TAGGED

リソースタイプ： AWS::CustomerProfiles::ObjectType

トリガータイプ: 設定変更

AWS リージョン： アフリカ (ケープタウン) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部

(オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

custom-eventbus-policy-attached

Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされているかどうかを確認します。カスタムイベントバスポリシーにリソースベースのポリシーがアタッチされていない場合、ルールは NON_COMPLIANT です。

識別子: CUSTOM_EVENTBUS_POLICY_ATTACHED

リソースタイプ: AWS::Events::EventBus

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

custom-schema-registry-policy-attached

カスタム Amazon EventBridge スキーマレジストリにリソースポリシーがアタッチされているかどうかを確認します。リソースポリシーがアタッチされていないカスタムスキーマレジストリの場合、ルールは NON_COMPLIANT です。

識別子: CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

リソースタイプ: AWS::EventSchemas::Registry

トリガータイプ: 定期的

AWS リージョン： 欧州 (ストックホルム) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、アジアパシフィック (香港) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

cw-loggroup-retention-period-check

Amazon CloudWatch ロググループの保持期間が 365 日を上回る日数または特定の保持期間に設定されているかどうかを確認します。保持期間が `MinRetentionTime` (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

> **Note**
> ロググループの保存設定が「期限なし」の場合、ルールは COMPLIANT としてマークされます。

識別子: CW_LOGGROUP_RETENTION_PERIOD_CHECK

リソースタイプ: AWS::Logs::LogGroup

トリガータイプ: 定期的

AWS リージョン： 中東 (アラブ首長国連邦) AWS リージョンを除く、サポートされているすべてのリージョン

パラメータ：

LogGroupNames (オプション), タイプ: CSV

保持期間を確認するための、ロググループ名のカンマ区切りリスト。

MinRetentionTime (オプション), タイプ: int

保持期間を日数で指定します。有効な値は 1、3、5、7、14、30、60、90、120、150、180、365、400、545、731、1827、3653 です。デフォルトの保持期間は 365 日間です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

datasync-task-data-verification-enabled

AWS DataSync タスクで、転送の終了時に追加の検証を実行するためのデータ検証が有効になっているかどうかを確認します。configuration.Options.VerifyMode が「NONE」の場合、ルールは NON_COMPLIANT です。

識別子： DATASYNC_TASK_DATA_VERIFICATION_ENABLED

リソースタイプ: AWS::DataSync::Task

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

datasync-task-logging-enabled

AWS DataSync タスクで Amazon CloudWatch ログ記録が有効になっているかどうかを確認します。 AWS DataSync タスクで Amazon CloudWatch ログ記録が有効になっていない場合、またはログ記録レベルが指定したログ記録レベルと等しくない場合、ルールは NON_COMPLIANT です。

識別子: DATASYNC_TASK_LOGGING_ENABLED

リソースタイプ: AWS::DataSync::Task

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

logLevel (オプション), タイプ: 文字列

ログレベルの文字列値。有効な値には、「BASIC」と「TRANSFER」が含まれます。指定されなかった場合、デフォルト値は「BASIC」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

datasync-task-tagged

AWS DataSync タスクにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： DATASYNC_TASK_TAGGED

リソースタイプ: AWS::DataSync::Task

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dax-encryption-enabled

Amazon DynamoDB Accelerator (DAX) クラスターが暗号化されているかどうかを確認します。DAX クラスターが暗号化されていない場合、ルールは NON_COMPLIANT です。

識別子: DAX_ENCRYPTION_ENABLED

リソースタイプ: AWS::DAX::Cluster

トリガータイプ: 定期的

AWS リージョン： 欧州 (ストックホルム) 、中国 (北京) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、欧州 (スペイン) 、中国 (寧夏) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dax-tls-endpoint-encryption

Amazon DynamoDB Accelerator (DAX) クラスターの ClusterEndpointEncryptionType が TLS に設定されているかどうかを確認します。DAX クラスターが Transport Layer Security (TLS) によって暗号化されていない場合、ルールは NON_COMPLIANT です。

識別子: DAX_TLS_ENDPOINT_ENCRYPTION

リソースタイプ: AWS::DAX::Cluster

[トリガータイプ:] 定期的

AWS リージョン: アジアパシフィック (ムンバイ)、欧州 (パリ)、米国東部 (オハイオ)、欧州 (アイルランド)、欧州 (フランクフルト)、南米 (サンパウロ)、米国東部 (バージニア北部)、欧州 (ロンドン)、アジアパシフィック (東京)、米国西部 (オレゴン)、米国西部 (北カリフォルニア)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

db-instance-backup-enabled

RDS DB インスタンスでバックアップが有効になっているかどうかを確認します。オプションで、バックアップ保存期間およびバックアップウィンドウを確認します。

識別子: DB_INSTANCE_BACKUP_ENABLED

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

backupRetentionPeriod (オプション), タイプ: int

バックアップ保持期間。

backupRetentionMinimum (オプション), タイプ: int

バックアップの最短保持期間

preferredBackupWindow (オプション), 型: 文字列

バックアップを作成する時間範囲。

checkReadReplicas (オプション), 型: ブール値

リードレプリカに対して RDS DB インスタンスでバックアップが有効になっているかどうかを確認します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

desired-instance-tenancy

EC2 インスタンスの「テナンシー」値を確認します。また、AMI ID がこれらの AMI から起動するように指定されているかどうか、ホスト ID がそれらの専用ホストから起動するように指定されているかどうかも確認します。インスタンスがリスト内のホストと AMI (指定されている場合) と一致する場合、ルールは COMPLIANT になります。

識別子: DESIRED_INSTANCE_TENANCY

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

tenancy, 型: 文字列

インスタンスの望ましいテナンシー 有効な値は、DEDICATED、HOST、および DEFAULT です。

imageId (オプション), タイプ: CSV

このルールは、指定された ID を持つ AMI から起動されたインスタンスのみを評価します。複数の AMI ID はカンマで区切ります。

hostId (オプション), タイプ: CSV

インスタンスの起動元となる EC2 専有ホストの ID。複数のホスト ID はカンマで区切ります。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

desired-instance-type

EC2 インスタンスが特定のインスタンスタイプであるかどうかを確認します。EC2 インスタンスがパラメータリストで指定されていない場合、ルールは NON_COMPLIANT です。サポートされる

EC2 インスタンスタイプのリストについては、Linux インスタンス用の EC2 ユーザーガイドのインスタンスタイプを参照してください。

識別子: DESIRED_INSTANCE_TYPE

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

instanceType, タイプ: CSV

EC2 インスタンスタイプのカンマ区切りリスト (例: "t2.small, m4.large, i2.xlarge")。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-auto-minor-version-upgrade-check

AWS Database Migration Service (AWS DMS) レプリケーションインスタンスで自動マイナーバージョンアップグレードが有効になっているかどうかを確認します。 AWS DMS レプリケーションインスタンスにマイナーバージョンの自動アップグレードが設定されていない場合、ルールは NON_COMPLIANT です。

識別子: DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

リソースタイプ: AWS::DMS::ReplicationInstance

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、

欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべてのリージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-endpoint-ssl-configured

AWS Database Migration Service (AWS DMS) エンドポイントが SSL 接続で設定されているかどうかを確認します。DMS に SSL AWS 接続が設定されていない場合、ルールは NON_COMPLIANT です。

コンテキスト: SSL/TLS 接続は、クライアントと DB インスタンスの間を移動するデータを暗号化することによって、1 つのセキュリティ層を提供します。サーバー証明書を使用すると、Amazon RDS DB インスタンスへの接続が確立されていることを検証することによって、追加のセキュリティレイヤーが提供されます。これを行うには、プロビジョニングしたすべての DB インスタンスに自動インストールされたサーバー証明書をチェックします。で SSL 接続を有効にすることで AWS DMS、移行中のデータの機密性を保護します。

の SSL 接続を設定するには AWS DMS、Amazon Relational Database Service ユーザーガイド」の「[SSL/TLS を使用して DB インスタンスまたはクラスターへの接続を暗号化する](#)」を参照してください。

識別子: DMS_ENDPOINT_SSL_CONFIGURED

リソースタイプ: AWS::DMS::Endpoint

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシ

コ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべてのリージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-endpoint-tagged

DMS AWS エンドポイントにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： DMS_ENDPOINT_TAGGED

リソースタイプ: AWS::DMS::Endpoint

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-mongo-db-authentication-enabled

MongoDb データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、パスワードベースの認証とアクセスコントロールが有効になっているかどうかを確認します。パスワードベースの認証とアクセスコントロールが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: DMS_MONGO_DB_AUTHENTICATION_ENABLED

リソースタイプ: AWS::DMS::Endpoint

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-neptune-iam-authorization-enabled

Amazon Neptune AWS データベースの Database Migration Service (AWS DMS) エンドポイントが IAM 認可で設定されているかどうかを確認します。Neptune がターゲットである DMS AWS エンドポイントで IamAuthEnabled が false に設定されている場合、ルールは NON_COMPLIANT です。

識別子: DMS_NEPTUNE_IAM_AUTHORIZATION_ENABLED

リソースタイプ: AWS::DMS::Endpoint

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-redis-tls-enabled

Redis データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、他のエンドポイントと通信されるデータの TLS/SSL 暗号化が有効になっているかどうかを確認します。TLS/SSL が有効でない場合、ルールは NON_COMPLIANT です。

識別子: DMS_REDIS_TLS_ENABLED

リソースタイプ: AWS::DMS::Endpoint

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-replication-not-public

AWS Database Migration Service (AWS DMS) レプリケーションインスタンスがパブリックかどうかを確認します。PubliclyAccessible フィールドが true に設定されている場合、ルールは NON_COMPLIANT です。

識別子: DMS_REPLICATION_NOT_PUBLIC

リソースタイプ: AWS::DMS::ReplicationInstance

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-replication-task-sourcedb-logging

ソースデータベースの DMS AWS レプリケーションタスクの有効な重要度レベルでログ記録が有効になっているかどうかを確認します。ログ記録が有効にされていない場合、またはソースデータベースの DMS レプリケーションタスクのログの重要度レベルが有効でもない場合、ルールは NON_COMPLIANT です。

識別子: DMS_REPLICATION_TASK_SOURCEDB_LOGGING

リソースタイプ: AWS::DMS::ReplicationTask

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-replication-task-tagged

DMS AWS レプリケーションタスクにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： DMS_REPLICATION_TASK_TAGGED

リソースタイプ: AWS::DMS::ReplicationTask

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dms-replication-task-targetdb-logging

ターゲットデータベースの DMS AWS レプリケーションタスクイベントの有効な重要度レベルでログ記録が有効になっているかどうかを確認します。ログ記録が有効にされていない場合、またはターゲットデータベースのレプリケーションタスクのログ記録の重要度レベルが有効でもない場合、ルールは NON_COMPLIANT です。

識別子: DMS_REPLICATION_TASK_TARGETDB_LOGGING

リソースタイプ: AWS::DMS::ReplicationTask

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

docdb-cluster-audit-logging-enabled

Amazon DocumentDB (MongoDB 互換) インスタンスクラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっているかどうかを確認します。Amazon DocumentDB インスタンスクラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、米国西部 (北カリフォルニア) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

docdb-cluster-backup-retention-check

Amazon Document DB クラスターの保持期間が特定の日数に設定されているかどうかを確認します。保持期間がパラメータで指定された値よりも短い場合、ルールは NON_COMPLIANT です。

識別子: DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、米国西部 (北カリフォルニア) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

minimumBackupRetentionPeriod (オプション), タイプ: int

最低日数のバックアップを保存する必要があります。有効な値は 1 ~ 35 で、デフォルト値は 7 です。値が「backupRetentionPeriod」より大きい場合、このルールは NON_COMPLIANT です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

docdb-cluster-deletion-protection-enabled

Amazon DocumentDB (MongoDB 互換) クラスターで削除保護が有効になっているかどうかを確認します。Amazon DocumentDB クラスターの deletionProtection フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

識別子: DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、米国西部 (北カリフォルニア) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

docdb-cluster-encrypted

Amazon DocumentDB (MongoDB 互換) クラスターでストレージ暗号化が有効になっているかどうかを確認します。ストレージの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: DOCDB_CLUSTER_ENCRYPTED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、米国西部 (北カリフォルニア) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

kmsKeyArns (オプション), タイプ: CSV

> 暗号化されたクラスターの KmsKeyID と比較するための KMS キー ARN のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

docdb-cluster-encrypted-in-transit

Amazon DocumentDB クラスターへの接続が転送中の暗号化を使用するように設定されているかどうかを確認します。パラメータグループが「同期中」でない場合、または TLS パラメータが「無効」または の値に設定されている場合、ルールは NON_COMPLIANT ですexcludeTlsParameters。

識別子： DOCDB_CLUSTER_ENCRYPTED_IN_TRANSIT

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 定期的

AWS リージョン： 欧州 (ストックホルム) 、中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、米国西部 (北カリフォルニア) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

excludeTlsParameters (オプション) , タイプ: CSV

> チェックしないルールの TLS クラスターパラメータのカンマ区切りリスト。デフォルト値: 'disabled'。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

docdb-cluster-snapshot-public-prohibited

Amazon DocumentDB 手動クラスタースナップショットがパブリックかどうかを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。

識別子: DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROBICTED

リソースタイプ: AWS::RDS::DBClusterSnapshot

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、中東 (アラブ首長国連邦) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、アジアパシフィック (香港) 、アジアパシフィック (ハイデラバード) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、欧州 (ミラノ) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能です。

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dynamodb-autoscaling-enabled

Amazon DynamoDB テーブルまたはグローバルセカンダリインデックスが、Auto Scaling が有効なオンデマンドモードまたはプロビジョニングモードを使用して、読み取り/書き込み容量を処理できるかどうかを確認します。Auto Scaling が有効でない場合、ルールは NON_COMPLIANT です。

識別子: DYNAMODB_AUTOSCALING_ENABLED

リソースタイプ: AWS::DynamoDB::Table

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

minProvisionedReadCapacity (オプション), タイプ: int

> Auto Scaling グループで、読み取りキャパシティーによりプロビジョニングするユニットの最小数。

maxProvisionedReadCapacity (オプション), タイプ: int

Auto Scaling グループで、読み取りキャパシティーによりプロビジョニングするユニットの最大数。

targetReadUtilization (オプション), 型: 倍精度浮動小数点数

読み込みキャパシティーのターゲット使用率 (%)。ターゲット使用率は、プロビジョニングされたキャパシティーに対する消費されたキャパシティーの割合で示されます。

minProvisionedWriteCapacity (オプション), タイプ: int

Auto Scaling グループで、書き込みキャパシティーによりプロビジョニングするユニットの最小数。

maxProvisionedWriteCapacity (オプション), タイプ: int

Auto Scaling グループで、書き込みキャパシティーによりプロビジョニングするユニットの最大数。

targetWriteUtilization (オプション), 型: 倍精度浮動小数点数

書き込みキャパシティーのターゲット使用率 (%)。ターゲット使用率は、プロビジョニングされたキャパシティーに対する消費されたキャパシティーの割合で示されます。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dynamodb-in-backup-plan

Amazon DynamoDB テーブルが AWS Backup Plans に存在するかどうかを確認します。Amazon DynamoDB テーブルが AWS Backup プランに存在しない場合、ルールは NON_COMPLIANT です。

識別子: DYNAMODB_IN_BACKUP_PLAN

リソースタイプ: AWS::DynamoDB::Table

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dynamodb-last-backup-recovery-point-created

Amazon DynamoDB テーブルのリカバリポイントが指定した期間内に作成されたかどうかを確認します。DynamoDB テーブルに対応するリカバリポイントが指定した期間内に作成されていない場合、ルールは NON_COMPLIANT です。

識別子: DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::DynamoDB::Table

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの DynamoDB テーブルのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

チェックするルールの DynamoDB テーブルの名前。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dynamodb-meets-restore-time-target

Amazon DynamoDB テーブルの復元時間が、指定された期間と一致しているかどうかを確認します。DynamoDB テーブルの LatestRestoreExecutionTimeMinutes が maxRestoreTime の値より大きい場合、ルールは NON_COMPLIANT です。

識別子: DYNAMODB_MEETS_RESTORE_TIME_TARGET

リソースタイプ: AWS::DynamoDB::Table

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

maxRestoreTime, タイプ: int

最大許容復元ランタイムの数値。

resourceTags (オプション), 型: 文字列

チェックするルールの DynamoDB テーブルのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

チェックするルールの DynamoDB テーブルの名前。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dynamodb-pitr-enabled

ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっているかどうかを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: DYNAMODB_PITR_ENABLED

リソースタイプ: AWS::DynamoDB::Table

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

DynamoDB-バックアップ計画によって保護されるリソース

Amazon DynamoDB テーブルがバックアップ計画で保護されているかどうかを確認します。DynamoDB テーブルがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

識別子:DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

リソースタイプ: AWS::DynamoDB::Table

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

resourceTags (オプション), 型: 文字列

チェックするルールの DynamoDB テーブルのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

チェックするルールの DynamoDB テーブルの名前。

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dynamodb-table-deletion-protection-enabled

Amazon DynamoDB テーブルの削除保護が有効に設定されているかどうかを確認します。テーブルの削除保護が無効になっている場合、ルールは NON_COMPLIANT です。

識別子: DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

リソースタイプ: AWS::DynamoDB::Table

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dynamodb-table-encrypted-kms

Amazon DynamoDB テーブルが AWS Key Management Service (KMS) で暗号化されているかどうかを確認します。Amazon DynamoDB テーブルが KMS で暗号化されていない場合、ルールは NON_COMPLIANT AWS です。暗号化された KMS キーが`kmsKeyArns`入力パラメータに存在しない場合も、ルールは NON_COMPLIANT AWS です。

識別子: DYNAMODB_TABLE_ENCRYPTED_KMS

リソースタイプ: AWS::DynamoDB::Table

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

kmsKeyArns (オプション), タイプ: CSV

> Amazon DynamoDB テーブルの暗号化に使用できる AWS KMS キー ARNs のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dynamodb-table-encryption-enabled

Amazon DynamoDB テーブルが暗号化されているかどうか、およびそのステータスを確認します。ステータスが有効または有効化中の場合、ルールは COMPLIANT です。

識別子: DYNAMODB_TABLE_ENCRYPTION_ENABLED

リソースタイプ: AWS::DynamoDB::Table

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、中東 (バーレーン) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、アジアパシフィック (香港) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、欧州 (ミラノ) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

dynamodb-throughput-limit-check

DynamoDB のプロビジョンドスループットがアカウントの上限に近づいているかどうかを確認します。デフォルトでは、このルールはプロビジョンドスループットがアカウント上限の 80% のしきい値を超えているかどうかを確認します。

識別子: DYNAMODB_THROUGHPUT_LIMIT_CHECK

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

accountRCUThresholdPercentage (オプション), タイプ: int, デフォルト: 80

アカウントのプロビジョンド読み込みキャパシティー単位の割合 (%)。この値に到達すると、ルールは非準拠とマークされます。

accountWCUThresholdPercentage (オプション), タイプ: int, デフォルト: 80

アカウントのプロビジョンド書き込みキャパシティー単位の割合 (%)。この値に到達すると、ルールは非準拠とマークされます。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ebs-in-backup-plan

Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup のバックアッププランに追加されているかどうかを確認します。Amazon EBS ボリュームが Backup プランに含まれていない場合、ルールは NON_COMPLIANT です。

識別子: EBS_IN_BACKUP_PLAN

リソースタイプ: AWS::EC2::Volume

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (メルボルン) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ebs-last-backup-recovery-point-created

Amazon Elastic Block Store (Amazon EBS) のリカバリポイントが作成されたかどうかを確認します。Amazon EBS ボリュームに対応するリカバリポイントが指定した期間内に作成されていない場合、ルールは NON_COMPLIANT です。

識別子: EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::EC2::Volume

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EBS ボリュームのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon EBS ボリュームの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ebs-meets-restore-time-target

Amazon Elastic Block Store (Amazon EBS) ボリュームの復元時間が、指定された期間と一致しているかどうかを確認します。Amazon EBS ボリュームの LatestRestoreExecutionTimeMinutes が maxRestoreTime の値より大きい場合、ルールは NON_COMPLIANT です。

識別子: EBS_MEETS_RESTORE_TIME_TARGET

リソースタイプ: AWS::EC2::Volume

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

maxRestoreTime, タイプ: int

最大許容復元ランタイムの数値。

resourceTags (オプション), タイプ: 文字列

チェックするルールの Amazon EBS ボリュームのタグ (JSON 形式) 。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon EBS ボリュームの ID。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ebs-optimized-instance

Amazon EBS 最適化できる Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに対して Amazon EBS 最適化が有効になっているかどうかを確認します。EBS 最適化が可能な AmazonEC2 インスタンスに対して EBS 最適化が有効化されていない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> デフォルトで EBS に最適化されている EC2 インスタンスでは、常にルール評価で `COMPLIANT` が返されます。

識別子: EBS_OPTIMIZED_INSTANCE

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ebs-resources-in-logically-air-gapped-vault

Amazon Elastic Block Store (Amazon EBS) ボリュームが論理エアギャップボールトにあるかどうかを確認します。Amazon EBS ボリュームが指定された期間内に論理エアギャップボールトにない場合、ルールは NON_COMPLIANT です。

識別子: EBS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

リソースタイプ: AWS::EC2::Volume

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各 AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EBS ボリュームのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon EBS ボリュームの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 2184 以下、日は 91 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

バックアップ計画によって保護された EBS リソース

Amazon Elastic Block Store (Amazon EBS) ボリュームが、バックアップ計画に追加されているかどうかを確認します。Amazon EBSボリュームがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

識別子:EBS_RESOURCES_PROTECTED_BACKUP_PLAN

リソースタイプ: AWS::EC2::Volume

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EBS ボリュームのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon EBS ボリュームの ID。

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ebs-snapshot-public-restorable-check

Amazon Elastic Block Store (Amazon EBS) スナップショットがパブリックに復元不可能になっているかどうかを確認します。RestorableByUserIds フィールドを持つ 1 つ以上のスナップショットが

「all」に設定されている場合、つまり Amazon EBS スナップショットがパブリックである場合、ルールは NON_COMPLIANT です。

識別子: EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

トリガータイプ: 定期的

AWS リージョン： 欧州 (スペイン) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-capacity-reservation-tagged

Amazon EC2 キャパシティ予約にタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_CAPACITY_RESERVATION_TAGGED

リソースタイプ： AWS::EC2::CapacityReservation

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-carrier-gateway-tagged

Amazon EC2 キャリアゲートウェイにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_CARRIER_GATEWAY_TAGGED

リソースタイプ： AWS::EC2::CarrierGateway

トリガータイプ: 設定変更

AWS リージョン： 欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-client-vpn-connection-log-enabled

AWS クライアント VPN エンドポイントでクライアント接続のログ記録が有効になっているかどうかを確認します。「Configuration.ConnectionLogOptions.Enabled」が False に設定されている場合、ルールは NON_COMPLIANT です。

識別子: EC2_CLIENT_VPN_CONNECTION_LOG_ENABLED

リソースタイプ: AWS::EC2::ClientVpnEndpoint

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-client-vpn-endpoint-tagged

Amazon EC2 クライアント VPN エンドポイントにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_CLIENT_VPN_ENDPOINT_TAGGED

リソースタイプ: AWS::EC2::ClientVpnEndpoint

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-client-vpn-not-authorize-all

AWS クライアント VPN 認可ルールがすべてのクライアントの接続アクセスを許可するかどうかを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。

識別子: EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL

リソースタイプ: AWS::EC2::ClientVpnEndpoint

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-dhcp-options-tagged

Amazon EC2 DHCP オプションにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_DHCP_OPTIONS_TAGGED

リソースタイプ： AWS::EC2::DHCPOptions

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-ebs-encryption-by-default

Amazon Elastic Block Store (EBS) 暗号化がデフォルトで有効になっているかどうかを確認します。暗号化が有効でない場合、ルールは NON_COMPLIANT です。

識別子: EC2_EBS_ENCRYPTION_BY_DEFAULT

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-enis-source-destination-check-enabled

ユーザーによって管理される EC2 ENIs で送信元/送信先チェックが有効になっているかどうかを確認します。これらの ENIs」、「aws_codestar_connections_managed」、「branch」、「efa」、「interface」、「quicksight」のソース/宛先チェックが無効になっている場合、ルールは NON_COMPLIANT です。

識別子： EC2_ENIS_SOURCE_DESTINATION_CHECK_ENABLED

リソースタイプ： AWS::EC2::NetworkInterface

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (ソウル) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-fleet-tagged

Amazon EC2 フリートにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_FLEET_TAGGED

リソースタイプ： AWS::EC2::EC2Fleet

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-imdsv2-check

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのメタデータのバージョンが、Instance Metadata Service Version 2 (IMDSv2) で設定されているかどうかを確認します。HttpTokens が「optional」に設定されている場合、ルールは NON_COMPLIANT です。

識別子: EC2_IMDSV2_CHECK

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-instance-detailed-monitoring-enabled

詳細モニタリングが EC2 インスタンスに対して有効になっているかどうかを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: EC2_INSTANCE_DETAILED_MONITORING_ENABLED

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-instance-launched-with-allowed-ami

実行中または停止中の EC2 インスタンスが、許可された AMIs 基準を満たす Amazon マシンイメージ (AMIs) で起動されたかどうかを確認します。AMI が許可された AMI 基準を満たしておらず、許可された AMIs 設定が無効になっていない場合、ルールは NON_COMPLIANT AMIs。

識別子： EC2_INSTANCE_LAUNCHED_WITH_ALLOWED_AMI

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更および定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

InstanceStateNameList (オプション) , タイプ: CSV

チェックするルールの Amazon EC2 インスタンス状態のカンマ区切りリスト。有効な値は「実行中」と「停止」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-instance-managed-by-systems-manager

> **Important**
>
> このルールでは、ルール識別子 (EC2_INSTANCE_MANAGED_BY_SSM) とルール名 (ec2-instance-managed-by-systems-manager) が異なります。

Amazon EC2 インスタンスが AWS Systems Manager エージェント (SSM エージェント) によって管理されているかどうかを確認します。EC2 インスタンスが実行されていて SSM エージェントを停止している場合、または EC2 インスタンスが実行されていて SSM エージェントが終了している場合、ルールは NON_COMPLIANT です。

> **Note**
>
> EC2 インスタンスが停止して、SSM エージェントが実行されている場合、ルールは NON_COMPLIANT を返しません。

識別子: EC2_INSTANCE_MANAGED_BY_SSM

リソースタイプ: AWS::EC2::Instance、AWS::SSM::ManagedInstanceInventory

トリガータイプ: 設定変更

AWS リージョン： 中東 (アラブ首長国連邦) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-instance-multiple-eni-check

Amazon Elastic Compute Cloud (Amazon EC2) で複数の Elastic Network Interfaces (ENI) または Elastic Fabric Adapters (EFA) が使用されているかどうかを確認します。Amazon EC2 インスタンスで複数のネットワークインターフェイスが使用されている場合、ルールは NON_COMPLIANT です。

識別子: EC2_INSTANCE_MULTIPLE_ENI_CHECK

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

NetworkInterfaceIds (オプション), タイプ: CSV

ネットワークインスタンス ID のカンマ区切りリスト

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、[AWS Config 「ルールを使用したリソースの評価」](#)を参照してください。このルールがプロアクティブモードで COMPLIANT を返すに

は、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

ec2-instance-no-public-ip

EC2 インスタンスにパブリック IP の関連付けがあるかどうかを確認します。EC2 インスタンスの設定項目に publicIp フィールドが存在する場合、ルールは NON_COMPLIANT です。ルールは、IPv4 のみに適用されます。

コンテキスト: パブリック IP アドレスにより EC2 インスタンスにインターネットから直接アクセスできるようになりますが、これはセキュリティやコンプライアンスの観点からは必ずしも望ましいことではありません。

- セキュリティ: 多くの場合、パブリックにアクセス可能にする必要がない限り、EC2 インスタンスにパブリック IP アドレスを持たせることはありません。パブリック IP アドレスを持たせると、EC2 インスタンスが不正アクセスや攻撃などの潜在的なセキュリティリスクにさらされる可能性があります。
- コンプライアンス: PCI、DSS、HIPAA などのさまざまなコンプライアンス標準には、ネットワークセグメンテーションとアクセス制御に関する特定の要件があります。EC2 インスタンスに不要なパブリック IP アドレスが割り当てられないようにすることで、これらの要件を確実に順守できます。
- コスト管理: パブリック IP アドレスには、特に EC2 インスタンスが継続的に関連付けられている場合、追加コストが発生する可能性があります。必要のないパブリック IP を持つ EC2 インスタンスを特定することで、コストを削減できる可能性があります。

Identifier: EC2_INSTANCE_NO_PUBLIC_IP

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-instance-profile-attached

EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされているかどうかを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

識別子: EC2_INSTANCE_PROFILE_ATTACHED

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

IamInstanceProfileArnList (オプション), タイプ: CSV

Amazon EC2 インスタンスにアタッチできる IAM プロファイルの Amazon リソースネーム (ARN) のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-last-backup-recovery-point-created

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのリカバリポイントが作成されたかどうかを確認します。Amazon EC2 インスタンスに対応するリカバリポイントが指定した期間内に作成されていない場合、ルールは NON_COMPLIANT です。

識別子: EC2_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EC2 インスタンスのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

ルールの Amazon EC2 インスタンスの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-launch-template-imdsv2-check

現在設定されている Amazon EC2 起動テンプレートのデフォルトバージョンで、Amazon EC2 インスタンスメタデータサービス (IMDSv2) の V2 を使用するために、新しく起動されたインスタンスが必要かどうかを確認します。「メタデータバージョン」が V2 (IMDSv2) として指定されていない場合、ルールは NON_COMPLIANT です。

識別子: EC2_LAUNCH_TEMPLATE_IMDSV2_CHECK

リソースタイプ: AWS::EC2::LaunchTemplate

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-launch-template-public-ip-disabled

Amazon EC2 起動テンプレートが、ネットワークインターフェイスにパブリック IP アドレスを割り当てるように設定されているかどうかを確認します。EC2 起動テンプレートのデフォルトバージョンで、「AssociatePublicIpAddress」が「true」に設定されているネットワークが 1 つまたは複数ある場合、ルールは NON_COMPLIANT です。

識別子: EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

リソースタイプ: AWS::EC2::LaunchTemplate

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

exemptedLaunchTemplates (オプション), タイプ: CSV

除外された EC2 起動テンプレート ID リスト (カンマ区切り) で、 AssociatePublicIpAddress の値が「true」に設定されたネットワークインターフェイスを使用可能なもの。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-launch-template-tagged

Amazon EC2 起動テンプレートにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_LAUNCH_TEMPLATE_TAGGED

リソースタイプ: AWS::EC2::LaunchTemplate

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエ

ル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-managedinstance-applications-blacklisted

指定したアプリケーションのいずれもインスタンスにインストールされていないかどうかを確認します。必要に応じて、バージョンを指定します。新しいバージョンは拒否リストに記載されません。オプションで、プラットフォームを指定すると、このプラットフォームを実行しているインスタンスにのみルールが適用されます。

識別子: EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

リソースタイプ: AWS::SSM::ManagedInstanceInventory

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

applicationNames, タイプ: CSV

アプリケーション名のカンマ区切りリスト。必要に応じて、バージョンに ":" を追加します (例: 'Chrome:0.5.3, Firefox')。

> **Note**
>
> アプリケーション名は完全に一致する必要があります。例えば、Linux で **`firefox`** または Amazon Linux で **`firefox-compat`** を使用します。さらに、 は現在 applicationNames パラメータ (など) のワイルドカードをサポート AWS Config していません**`firefox*`**。

platformType (オプション), 型: 文字列

プラットフォームタイプ (例: 'Linux' または 'Windows')。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-managedinstance-applications-required

すべての指定したアプリケーションが、インスタンスにインストールされているかどうかを確認します。オプションで、使用可能な最小バージョンを指定します。また、そのプラットフォームを実行中のインスタンスのみにルールを適用するプラットフォームを指定できます。

> **Note**
>
> SSM エージェントが EC2 インスタンスで実行されており、アプリケーションソフトウェアインベントリを収集するための関連付けが作成されていることを確認します。`NOT_APPLICABLE` SSM エージェントがインストールされていない場合、または関連付けがまだ作成または実行されていない場合、ルールは を返します。

識別子: EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

リソースタイプ: AWS::SSM::ManagedInstanceInventory

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

applicationNames, タイプ: CSV

アプリケーション名のカンマ区切りリスト。必要に応じて、バージョンに ":" を追加します (例: 'Chrome:0.5.3, Firefox')。

> **Note**
> アプリケーション名は完全に一致する必要があります。例えば、Linux で **`firefox`** または Amazon Linux で **`firefox-compat`** を使用します。さらに、 は現在 applicationNames パラメータ (など) のワイルドカードをサポート AWS Config していません**`firefox*`**。

platformType (オプション), 型: 文字列

プラットフォームタイプ (例: 'Linux' または 'Windows')。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-managedinstance-association-compliance-status-check

インスタンスでの関連付けの実行後に、 AWS Systems Manager の関連付けコンプライアンスのステータスが COMPLIANT または NON_COMPLIANT かどうかを確認します。フィールドステータスが COMPLIANT の場合は、ルールに準拠しています。関連付けの詳細については、「[関連付けとは何ですか?](#)」 を参照してください。

識別子: EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

リソースタイプ: AWS::SSM::AssociationCompliance

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジア

パシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-managedinstance-inventory-blacklisted

Amazon EC2 Systems Manager が管理するインスタンスが、ブラックリストに記載されたインベントリタイプを収集するように設定されているかどうかを確認します。

識別子: EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

リソースタイプ: AWS::SSM::ManagedInstanceInventory

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

inventoryNames, タイプ: CSV

Systems Manager インベントリタイプのカンマ区切りリスト ('AWS:Network, AWS:WindowsUpdate' など) 。

platformType (オプション), 型: 文字列

プラットフォームタイプ (例: 'Linux')。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-managedinstance-patch-compliance-status-check

インスタンスにパッチをインストールした後、 AWS Systems Manager のパッチコンプライアンスのコンプライアンスステータスが COMPLIANT または NON_COMPLIANT かどうかを確認します。フィールドステータスが COMPLIANT の場合は、ルールに準拠しています。

識別子: EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

リソースタイプ: AWS::SSM::PatchCompliance

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (大阪) 、欧州 (ミラノ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-managedinstance-platform-check

EC2 マネージドインスタンスの設定が希望どおりであるかどうかを確認します。

識別子: EC2_MANAGEDINSTANCE_PLATFORM_CHECK

リソースタイプ: AWS::SSM::ManagedInstanceInventory

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

platformType, 型: 文字列

プラットフォームタイプ (例: 'Linux')。

platformVersion (オプション), 型: 文字列

プラットフォームのバージョン (例: '2016.09')。

agentVersion (オプション), 型: 文字列

エージェントのバージョン (例: '2.0.433.0')。

platformName (オプション), 型: 文字列

プラットフォームのバージョン (例: '2016.09')

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-meets-restore-time-target

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの復元時間が、指定された期間と一致しているかどうかを確認します。Amazon EC2 インスタンスの LatestRestoreExecutionTimeMinutes が maxRestoreTime の値より大きい場合、ルールは NON_COMPLIANT です。

識別子: EC2_MEETS_RESTORE_TIME_TARGET

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

maxRestoreTime, タイプ: int

最大許容復元ランタイムの数値。

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EC2 インスタンスのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

ルールの Amazon EC2 インスタンスの ID。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-network-insights-access-scope-analysis-tagged

Amazon EC2 ネットワークインサイトアクセススコープ分析にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_NETWORK_INSIGHTS_ACCESS_SCOPE_ANALYSIS_TAGGED

リソースタイプ： AWS::EC2::NetworkInsightsAccessScopeAnalysis

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-network-insights-access-scope-tagged

Amazon EC2 ネットワークインサイトのアクセススコープにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_NETWORK_INSIGHTS_ACCESS_SCOPE_TAGGED

リソースタイプ： AWS::EC2::NetworkInsightsAccessScope

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

EC2-network-insights-path-tagged

Amazon EC2 ネットワークインサイトパスにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_NETWORK_INSIGHTS_PATH_TAGGED

リソースタイプ： AWS::EC2::NetworkInsightsPath

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-no-amazon-key-pair

Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されているかどうかを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。

識別子: EC2_NO_AMAZON_KEY_PAIR

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-paravirtual-instance-check

EC2 インスタンスの仮想化タイプが準仮想化かどうかをチェックします。「virtualizationType」が「paravirtual」に設定されている場合、EC2 インスタンスのこのルールは NON_COMPLIANT です。

識別子: EC2_PARAVIRTUAL_INSTANCE_CHECK

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン: 中国 (北京)、欧州 (アイルランド)、欧州 (フランクフルト)、南米 (サンパウロ)、米国東部 (バージニア北部)、アジアパシフィック (東京)、米国西部 (オレゴン)、米国西部 (北カリフォルニア)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー) リージョンのみで利用可能です。

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-prefix-list-tagged

Amazon EC2 マネージドプレフィックスリストにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_PREFIX_LIST_TAGGED

リソースタイプ： AWS::EC2::PrefixList

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-resources-in-logically-air-gapped-vault

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスが論理エアギャップボールトにあるかどうかを確認します。Amazon EC2 インスタンスが指定された期間内に論理エアギャップボールトにない場合、ルールは NON_COMPLIANT です。

識別子: EC2_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各 AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EC2 インスタンスのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

ルールの Amazon EC2 インスタンスの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 2184 以下、日は 91 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-resources-protected-by-backup-plan

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスがバックアップ計画で保護されているかどうかを確認します。Amazon EC2 インスタンスがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> このルールは、Amazon EC2 インスタンスの実行にのみ適用され、パワーダウンされたインスタンスには適用されません。

識別子:EC2_RESOURCES_PROTECTED_BACKUP_PLAN

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EC2 インスタンスのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

ルールの Amazon EC2 インスタンスの ID。

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-security-group-attached-to-eni

デフォルトではないセキュリティグループが Elastic Network Interface にアタッチされているかどうかを確認します。そのセキュリティグループがネットワークインターフェイスに関連付けられていない場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): EC2_SECURITY_GROUP_ATTACHED_TO_ENI

リソースタイプ: AWS::EC2::SecurityGroup

トリガータイプ: 設定変更

AWS リージョン： AWS 中東 (アラブ首長国連邦) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-security-group-attached-to-eni-periodic

デフォルトではないセキュリティグループが Elastic Network Interface (ENI) にアタッチされているかどうかを確認します。そのセキュリティグループが ENI に関連付けられていない場合、ルールは NON_COMPLIANT になります。呼び出し元アカウントが所有していないセキュリティグループは NOT_APPLICABLE と評価されます。

> **Note**
>
> このルールは、`AWS::EC2::SecurityGroup` リソースタイプについて報告します。ただし、ルールを効果的に実行するには、`AWS::EC2::NetworkInterface` リソースタイプの記録を有効にする必要があります。

[Identifier] (識別子): EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC

リソースタイプ: AWS::EC2::SecurityGroup

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-spot-fleet-request-ct-encryption-at-rest

Amazon EC2 スポットフリートリクエストで、起動したすべての EC2 インスタンスの Amazon Elastic Block Store (Amazon EBS) ボリュームが暗号化されているかどうかを確認します。保管時に EBS ボリュームのいずれかが暗号化されていない場合、ルールは NON_COMPLIANT です。

識別子： EC2_SPOT_FLEET_REQUEST_CT_ENCRYPTION_AT_REST

リソースタイプ： AWS::EC2::SpotFleet

トリガータイプ: 設定変更

AWS リージョン： 欧州 (アイルランド) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、米国西部 (オレゴン) 、中国 (寧夏) 、欧州 (チューリッヒ) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-stopped-instance

許可されている日数よりも長く停止している Amazon Elastic Compute Cloud (Amazon EC2) インスタンスがあるかどうかを確認します。Amazon EC2 インスタンスの状態が、許可されている日数より長く停止している場合、またはその日数を判断できない場合、ルールは NON_COMPLIANT です。

識別子: EC2_STOPPED_INSTANCE

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 定期的

AWS リージョン： アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (大阪) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) 、カナダ西部 (カルガリー) AWS を除く、サポートされているすべての リージョン

パラメータ :

AllowedDays (オプション), タイプ: int, デフォルト: 30

> ルールが NON_COMPLIANT になる前に、Amazon EC2 インスタンスを停止できる日数。デフォルトの日数は 30 日です。

> **Note**
>
> このルールは収集された履歴データに依存するため、選択する日数は設定した保持期間より短くする必要があります。履歴データ保持の詳細については、AWS Config「データの削除」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

ec2-token-hop-limit-check

Amazon Elastic Compute Cloud (EC2) インスタンスメタデータに、希望する制限を下回る指定されたトークンホップ制限があるかどうかを確認します。ホップ制限値が意図した制限を超える場合、ルールはインスタンスに対して NON_COMPLIANT です。

識別子: EC2_TOKEN_HOP_LIMIT_CHECK

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

tokenHopLimit (オプション), タイプ: int

> 希望するトークンのホップ制限。有効な値は 1～64 です。どちらも含まれます。パラメータが指定されていない場合、デフォルト値は 1 です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-traffic-mirror-filter-description

Amazon EC2 トラフィックミラーフィルターに説明があるかどうかを確認します。configuration.Description が存在しない場合、ルールは NON_COMPLIANT です。

識別子： EC2_TRAFFIC_MIRROR_FILTER_DESCRIPTION

リソースタイプ： AWS::EC2::TrafficMirrorFilter

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-traffic-mirror-filter-tagged

Amazon EC2 トラフィックミラーフィルターにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_TRAFFIC_MIRROR_FILTER_TAGGED

リソースタイプ： AWS::EC2::TrafficMirrorFilter

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-traffic-mirror-session-description

Amazon EC2 トラフィックミラーセッションに説明があるかどうかを確認します。configuration.Description が存在しない場合、ルールは NON_COMPLIANT です。

識別子： EC2_TRAFFIC_MIRROR_SESSION_DESCRIPTION

リソースタイプ： AWS::EC2::TrafficMirrorSession

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-traffic-mirror-session-tagged

Amazon EC2 トラフィックミラーセッションにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_TRAFFIC_MIRROR_SESSION_TAGGED

リソースタイプ： AWS::EC2::TrafficMirrorSession

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

EC2-traffic-mirror-target-description

Amazon EC2 トラフィックミラーターゲットに説明があるかどうかを確認します。configuration.Description が存在しない場合、ルールは NON_COMPLIANT です。

識別子： EC2_TRAFFIC_MIRROR_TARGET_DESCRIPTION

リソースタイプ： AWS::EC2::TrafficMirrorTarget

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-traffic-mirror-target-tagged

Amazon EC2 トラフィックミラーターゲットにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_TRAFFIC_MIRROR_TARGET_TAGGED

リソースタイプ： AWS::EC2::TrafficMirrorTarget

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバー

ド) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-transit-gateway-auto-vpc-attach-disabled

Amazon Elastic Compute Cloud (Amazon EC2) トランジットゲートウェイで「AutoAcceptSharedAttachments」が有効になっているかどうかを確認します。「AutoAcceptSharedAttachments」が「有効」に設定されている場合、ルールは、トランジットゲートウェイに対して NON_COMPLIANT になります。

識別子: EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

リソースタイプ: AWS::EC2::TransitGateway

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-transit-gateway-multicast-domain-tagged

Amazon EC2 Transit Gateway マルチキャストドメインにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EC2_TRANSIT_GATEWAY_MULTICAST_DOMAIN_TAGGED

リソースタイプ： AWS::EC2::TransitGatewayMulticastDomain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-volume-inuse-check

EBS ボリュームが EC2 インスタンスにアタッチされているかどうかを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされるかどうかを確認します。

EBS ボリュームが、実行中の EC2 インスタンスにアタッチされている場合、ルールは COMPLIANT です。この場合、EC2 インスタンスが EBS ボリュームをアクティブ使用している場合、ルールは COMPLIANT です。

EBS ボリュームがどの EC2 インスタンスにもアタッチされていないか、停止または終了した EC2 インスタンスにアタッチされている場合、ルールは NON_COMPLIANT です。この場合、EC2 インスタンスが EBS ボリュームをアクティブに使用していない場合、ルールは NON_COMPLIANT です。

識別子: EC2_VOLUME_INUSE_CHECK

リソースタイプ: AWS::EC2::Volume

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

deleteOnTermination (オプション), 型: ブール値

> EBS ボリュームは、インスタンスの削除時に削除対象としてマークされます。可能な値: True または False (その他の入力値は NON_COMPLIANT としてマークされます)。`True` に設定されている場合、終了した EBS ボリュームが削除対象でない場合、ルールは NON_COMPLIANT です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-vpn-connection-logging-enabled

AWS Site-to-Site VPN 接続で、両方のトンネルで Amazon CloudWatch ログ記録が有効になっているかどうかを確認します。Site-to-Site VPN 接続のいずれかまたは両方のトンネルで CloudWatch ログが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: EC2_VPN_CONNECTION_LOGGING_ENABLED

リソースタイプ: AWS::EC2::VPNConnection

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecr-private-image-scanning-enabled

プライベート Amazon Elastic Container Registry (Amazon ECR) リポジトリでイメージスキャンが有効化されているかどうかを確認します。プライベート Amazon ECR リポジトリのスキャン頻度がプッシュ時のみスキャンまたは継続的スキャンでない場合、ルールは NON_COMPLIANT になります。イメージスキャンの有効化の詳細については、「Amazon ECR ユーザーガイド」の「[イメージスキャン](#)」を参照してください。

識別子: ECR_PRIVATE_IMAGE_SCANNING_ENABLED

リソースタイプ: AWS::ECR::Repository

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecr-private-lifecycle-policy-configured

プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されているかどうかを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

識別子 ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

リソースタイプ: AWS::ECR::Repository

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecr-private-tag-immutability-enabled

プライベート Amazon Elastic Container Registry (ECR) リポジトリでタグのイミュータビリティが有効化されているかどうかを確認します。プライベート ECR リポジトリに対してタグのイミュータビリティが有効化されていない場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

リソースタイプ: AWS::ECR::Repository

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecr-repository-cmk-encryption-enabled

ECR リポジトリがカスタマーマネージド KMS キーを使用して保管時に暗号化されているかどうかを確認します。リポジトリが AES256 またはデフォルトの KMS キー ('aws/ecr') を使用して暗号化されている場合、このルールは NON_COMPLIANT です。

識別子： ECR_REPOSITORY_CMK_ENCRYPTION_ENABLED

リソースタイプ: AWS::ECR::Repository

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

kmsKeyArns (オプション), タイプ: CSV

ECR リポジトリの暗号化を目的とした KMS キー Amazon リソースネーム (ARNs) のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecr-repository-tagged

Amazon ECR リポジトリにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： ECR_REPOSITORY_TAGGED

リソースタイプ: AWS::ECR::Repository

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-awsvpc-networking-enabled

アクティブな ECSTaskDefinitions のネットワークモードが、「awsvpc」に設定されているかどうかを確認します。アクティブな ECSTaskDefinitions が「awsvpc」に設定されていない場合、このルールは NON_COMPLIANT となります。

> **Note**
>
> このルールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

識別子: ECS_AWSVPC_NETWORKING_ENABLED

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-containers-nonprivileged

ECSTaskDefinitions のコンテナの定義内にある特権パラメータが「true」に設定されているかどうかを確認します。特権パラメータが「true」の場合、ルールは NON_COMPLIANT になります。

> **Note**
>
> このルールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

[Identifier] (識別子): ECS_CONTAINERS_NONPRIVILEGED

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-containers-readonly-access

Amazon Elastic Container Service (Amazon ECS) コンテナで、そのルートファイルシステムに対して読み取り専用アクセス権のみが設定されていることを確認します。ECSTaskDefinitions のコンテナの定義で readonlyRootFilesystem パラメータが「false」に設定されている場合、ルールは NON_COMPLIANT になります。

> **Note**
>
> このルールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

[Identifier] (識別子): ECS_CONTAINERS_READONLY_ACCESS

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-container-insights-enabled

Amazon Elastic Container Service クラスターでコンテナインサイトが有効になっているかどうかを確認します。コンテナインサイトが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: ECS_CONTAINER_INSIGHTS_ENABLED

リソースタイプ: AWS::ECS::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-fargate-latest-platform-version

ECS Fargate サービスが最新のプラットフォームバージョンに設定されているかどうかを確認します。Fargate 起動タイプの PlatformVersion が LATEST に設定されていない場合、またはパラメー

タとして LatestLinuxVersion も `latestWindowsVersion` も指定されていない場合、ルールは NON_COMPLIANT になります。

識別子: ECS_FARGATE_LATEST_PLATFORM_VERSION

リソースタイプ: AWS::ECS::Service

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

latestLinuxVersion (オプション), タイプ: 文字列

最新の Linux は、セマンティックバージョニング (SemVer) 形式の 'PlatformVersion' をサポートしていました。Fargate がデプロイされていて 'PlatformVersion' が明示的に指定されている場合、または CodeDeploy が 'DeploymentController' として使用されている場合は、パラメータが必要になることがあります

latestWindowsVersion (オプション), タイプ: 文字列

最新の Windows は、セマンティックバージョニング (SemVer) 形式の 'PlatformVersion' をサポートしていました。Fargate がデプロイされていて 'PlatformVersion' が明示的に指定されている場合、または CodeDeploy が 'DeploymentController' として使用されている場合は、パラメータが必要になることがあります

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-no-environment-secrets

シークレットがコンテナ環境変数として渡されるかどうかを確認します。1 つ、または複数の環境変数キーが「`secretKeys`」パラメータにリストされているキーに一致する場合、ルールは NON_COMPLIANT になります (Amazon S3 などの他の場所からの環境変数を除く)。

> **Note**
>
> このルールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

[Identifier] (識別子): ECS_NO_ENVIRONMENT_SECRETS

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

secretKeys, タイプ: CSV

タスク定義内のコンテナの定義の環境変数で検索するキー名のコンマ区切りのリストです。余分なスペースは削除されます。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-task-definition-log-configuration

アクティブな ECS タスクの定義に、logConfiguration が設定されているかどうかを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

> **Note**
>
> このルールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

識別子: ECS_TASK_DEFINITION_LOG_CONFIGURATION

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-task-definition-memory-hard-limit

Amazon Elastic Container Service (ECS) のタスク定義に、そのコンテナの定義に対するメモリ制限が設定されているかどうかを確認します。1 つのコンテナの定義に「memory」パラメータが存在しない場合、タスク定義のルールは NON_COMPLIANT になります。

> **Note**
>
> このルールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

[Identifier] (識別子): ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-task-definition-network-mode-not-host

Amazon ECS タスク定義の最新のアクティブなリビジョンがホストネットワークモードを使用しているかどうかを確認します。ECS タスク定義の最新のアクティブなリビジョンがホストネットワークモードを使用している場合、ルールは NON_COMPLIANT です。

識別子： ECS_TASK_DEFINITION_NETWORK_MODE_NOT_HOST

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-task-definition-nonroot-user

ECSTaskDefinitions が、実行先の Amazon Elastic Container Service (Amazon ECS) の EC2 起動タイプコンテナにユーザーを指定するかどうかを確認します。「user」パラメータが存在しない、または「root」に設定されている場合、ルールは NON_COMPLIANT になります。

> **Note**
>
> このルールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

[Identifier] (識別子): ECS_TASK_DEFINITION_NONROOT_USER

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-task-definition-pid-mode-check

ECSTaskDefinitions が、ホストのプロセス名前空間をその Amazon Elastic Container Service (Amazon ECS) コンテナと共有するように設定されているかどうかを確認します。pidMode パラメータが「host」に設定されている場合、ルールは NON_COMPLIANT になります。

> **Note**
>
> このルールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

[Identifier] (識別子): ECS_TASK_DEFINITION_PID_MODE_CHECK

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ecs-task-definition-user-for-host-mode-check

ホストネットワークモードの Amazon ECS タスク定義に、コンテナ定義に特権または非ルートがあるかどうかを確認します。タスク定義の最新のアクティブなリビジョンに privileged=false (または null) および user=root (または null) がある場合、ルールは NON_COMPLIANT です。

> **Important**
>
> ルールが準拠を返すには、1 つの条件のみを満たす必要があります
> このルールは、次のいずれかのシナリオで COMPLIANT です。
>
> - ネットワークモードがホストに設定されていない場合、
> - タスク定義の最新のアクティブなリビジョンに privileged=true がある場合、
> - タスク定義の最新のアクティブなリビジョンに、非ルートのユーザーがある場合。
>
> つまり、ルールが準拠を返すには、これらの条件の 1 つだけを満たす必要があります。タスク定義に privileged=true があるかどうかを具体的に確認するには、「ecs-containers-nonprivileged」を参照してください。タスク定義に非ルートのユーザーがあるかどうかを具体的に確認するには、「ecs-task-definition-nonroot-user」を参照してください。

識別子: ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

リソースタイプ: AWS::ECS::TaskDefinition

トリガータイプ: 設定変更

AWS リージョン： 中東 (アラブ首長国連邦) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

SkipInactiveTaskDefinitions (オプション), 型: ブール値

INACTIVE な Amazon EC2 タスクの定義を確認しないためのブールフラグ。「true」に設定すると、ルールは INACTIVE な Amazon EC2 タスクの定義を評価しません。「false」に設定すると、ルールは INACTIVE な Amazon EC2 タスクの定義の最新リビジョンを評価します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

efs-access-point-enforce-root-directory

Amazon Elastic File System (Amazon EFS) アクセスポイントが、ルートディレクトリを適用するよう設定されているかどうかを確認します。「Path」の値が「'/'」(ファイルシステムのデフォルトのルートディレクトリ) に設定されている場合、ルールは NON_COMPLIANT です。

識別子: EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

リソースタイプ: AWS::EFS::AccessPoint

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

approvedDirectories (オプション), タイプ: CSV

> Amazon EFS アクセスポイントのルートディレクトリの強制で承認されたサブディレクトリパスのカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

efs-access-point-enforce-user-identity

Amazon Elastic File System (Amazon EFS) アクセスポイントが、ユーザー ID を適用するよう設定されているかどうかを確認します。「PosixUser」が定義されていない場合、またはパラメータが提供され、対応するパラメータに一致するものがない場合、ルールは NON_COMPLIANT です。

識別子: EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

リソースタイプ: AWS::EFS::AccessPoint

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

approvedUids (オプション), タイプ: CSV

EFS アクセスポイントのユーザー適用で承認された POSIX ユーザー ID のカンマ区切りリスト。

approvedGids (オプション), タイプ: CSV

EFS アクセスポイントのユーザー適用で承認された POSIX グループ ID のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

efs-automatic-backups-enabled

Amazon Elastic File System (Amazon EFS) ファイルシステムの自動バックアップが有効になっているかどうかを確認します。「BackupPolicy.Status」が DISABLED に設定されている場合、ルールは NON_COMPLIANT です。

識別子: EFS_AUTOMATIC_BACKUPS_ENABLED

リソースタイプ: AWS::EFS::FileSystem

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

efs-encrypted-check

Amazon Elastic File System (Amazon EFS) が AWS Key Management Service () を使用してファイルデータを暗号化するように設定されているかどうかを確認しますAWS KMS。暗号化されたキーが `DescribeFileSystems` で false に設定されている場合、または `DescribeFileSystems` の `KmsKeyId` キーが `KmsKeyId` パラメータと一致 しない場合、ルールは NON_COMPLIANT です。

Identifier: EFS_ENCRYPTED_CHECK

リソースタイプ: AWS::EFS::FileSystem

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

KmsKeyId (オプション), 型: 文字列

EFS ファイルシステムの暗号化に使用される KMS キーの Amazon リソースネーム (ARN)。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

efs-filesystem-ct-encrypted

Amazon Elastic File System (Amazon EFS) が AWS Key Management Service (AWS KMS) でデータを暗号化するかどうかを確認します。ファイルシステムが暗号化されていない場合、ルールは NON_COMPLIANT です。任意で、ファイルシステムが指定された KMS キーで暗号化されていないかどうかを確認できます。

識別子: EFS_FILESYSTEM_CT_ENCRYPTED

リソースタイプ: AWS::EFS::FileSystem

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

kmsKeyArns (オプション), タイプ: 文字列

(オプション) KMS キーの Amazon リソースネーム (ARNs) AWS のカンマ区切りリスト。指定した場合、ルールは指定された KMS キーが Amazon EFS ファイルシステムを暗号化していないかどうかを確認します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

efs-in-backup-plan

Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup のバックアッププランに追加されているかどうかを確認します。EFS ファイルシステムがバックアッププランに含まれていない場合、ルールは NON_COMPLIANT です。

識別子: EFS_IN_BACKUP_PLAN

リソースタイプ: AWS::EFS::FileSystem

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

efs-last-backup-recovery-point-created

Amazon Elastic File System (Amazon EFS) ファイルシステムのリカバリポイントが作成されたかどうかを確認します。Amazon EFS ファイルシステムに対応するリカバリポイントが指定した期間内に作成されていない場合、ルールは NON_COMPLIANT です。

識別子: EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::EFS::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EFS ファイルシステムのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

チェックするルールの EFS ファイルシステムの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

efs-meets-restore-time-target

Amazon Elastic File System (Amazon EFS) ファイルシステムの復元時間が、指定された期間と一致しているかどうかを確認します。Amazon EFS ファイルシステムの LatestRestoreExecutionTimeMinutes が maxRestoreTime の値より大きい場合、ルールは NON_COMPLIANT です。

識別子: EFS_MEETS_RESTORE_TIME_TARGET

リソースタイプ: AWS::EFS::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

maxRestoreTime, タイプ: int

最大許容復元ランタイムの数値。

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EFS ファイルシステムのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

チェックするルールの EFS ファイルシステムの ID。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

efs-mount-target-public-accessible

Amazon Elastic File System (Amazon EFS) マウントターゲットがパブリックサブネットに関連付けられていないかどうかを確認します。Amazon EFS マウントターゲットがパブリックサブネットに関連付けられている場合、ルールは NON-COMPLIANT です。

識別子: EFS_MOUNT_TARGET_PUBLIC_ACCESSIBLE

リソースタイプ: AWS::EFS::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

efs-resources-in-logically-air-gapped-vault

Amazon Elastic File System (Amazon EFS) ファイルシステムが論理エアギャップボールトにあるかどうかを確認します。Amazon EFS ファイルシステムが指定された期間内に論理エアギャップボールトにない場合、ルールは NON_COMPLIANT です。

識別子: EFS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

リソースタイプ: AWS::EFS::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエ

ル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon EFS ファイルシステムのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

チェックするルールの EFS ファイルシステムの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 2184 以下、日は 91 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

バックアップ計画によって保護された efs リソース

Amazon Elastic File System (Amazon EFS) ファイルシステムがバックアップ計画で保護されているかどうかを確認します。EFS ファイルがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

識別子:RESOURCES_PROTECTED_BACKUP_PLAN

リソースタイプ: AWS::EFS::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの EFS ファイルシステムのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

ルールをチェックする EFS ファイルシステムの ID。

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

eip-attached

AWS アカウントに割り当てられたすべての Elastic IP アドレスが EC2 インスタンスまたは使用中の Elastic Network Interface にアタッチされているかどうかを確認します。Elastic IP アドレスの「AssociationId」が null の場合、ルールは NON_COMPLIANT です。

> **Note**
> 評価の結果が出るまでは最大 6 時間かかることがあります。

識別子: EIP_ATTACHED

リソースタイプ: AWS::EC2::EIP

トリガータイプ: 設定変更

AWS リージョン： 中東 (アラブ首長国連邦) AWS リージョンを除く、サポートされているすべてのリージョン

パラメータ：

なし

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

eks-cluster-logging-enabled

Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されているかどうかを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: EKS_CLUSTER_LOGGING_ENABLED

リソースタイプ: AWS::EKS::Cluster

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

eks-cluster-log-enabled

Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されているかどうかを確認します。Amazon EKS クラスターのログ記録が有効になっていない場合、またはログ記録が上記のログタイプを使用して有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: EKS_CLUSTER_LOG_ENABLED

リソースタイプ: AWS::EKS::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

logTypes (オプション), タイプ: CSV

チェックするルールの EKS クラスターコントロールプレーンログタイプのカンマ区切りリスト。有効な値: "api"、"audit"、"authenticator"、"controllerManager"、"scheduler

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

eks-cluster-oldest-supported-version

Amazon Elastic Kubernetes Service (EKS) クラスターが、サポートされているバージョンで最も古いものを実行しているかどうかを確認します。EKS クラスターがサポートされている最も古いバージョンを実行している場合 (パラメータ 「`oldestVersionSupported`」に等しい)、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

リソースタイプ: AWS::EKS::Cluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

oldestVersionSupported, タイプ: 文字列

AWSでサポートされている Kubernetes の最も古いバージョンの値です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

eks-cluster-secrets-encrypted

Amazon EKS クラスターが KMS を使用して暗号化された Kubernetes AWS シークレットを持つように設定されているかどうかを確認します。EKS クラスターに encryptionConfig リソースがない場合、または encryptionConfig がシークレットにリソースとして命名していない場合、このルールは NON_COMPLIANT です。

識別子: EKS_CLUSTER_SECRETS_ENCRYPTED

リソースタイプ: AWS::EKS::Cluster

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

kmsKeyArns (オプション), タイプ: CSV

EKS の使用が承認されている KMS キー Amazon リソースネーム (ARN)のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

eks-cluster-supported-version

Amazon Elastic Kubernetes Service (EKS) クラスターが、サポートされている Kubernetes バージョンを実行しているかどうかを確認します。サポートされていないバージョン (パラメータ「`oldestVersionSupported`」未満) を EKS クラスターが使用している場合、このルールは NON_COMPLIANT になります。

[Identifier] (識別子): EKS_CLUSTER_SUPPORTED_VERSION

リソースタイプ: AWS::EKS::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

oldestVersionSupported, タイプ: 文字列

AWSでサポートされている Kubernetes の最も古いバージョンの値です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

eks-endpoint-no-public-access

Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないかどうかを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

識別子: EKS_ENDPOINT_NO_PUBLIC_ACCESS

リソースタイプ: AWS::EKS::Cluster

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

eks-secrets-encrypted

Amazon Elastic Kubernetes Service クラスターが AWS Key Management Service (KMS) キーを使用して暗号化された Kubernetes シークレットを持つように設定されているかどうかを確認します。

- EKS クラスターにシークレットが含まれる encryptionConfig がリソースの 1 つとしてある場合、このルールは COMPLIANT です。
- EKS シークレットの暗号化に使用されるキーがパラメータと一致する場合も、このルールは COMPLIANT です。
- EKS クラスターに encryptionConfig がない場合、または encryptionConfig リソースにシークレットが含まれていない場合、このルールは NON_COMPLIANT です。
- EKS シークレットの暗号化に使用されるキーがパラメータと一致しない場合も、このルールは NON_COMPLIANT です。

識別子: EKS_SECRETS_ENCRYPTED

リソースタイプ: AWS::EKS::Cluster

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

kmsKeyArns (オプション), タイプ: CSV

EKS クラスター内の暗号化されたシークレットに使用する KMS キーの Amazon リソースネーム (ARN) のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache_automatic_backup_check_enabled

Amazon ElastiCache クラスター (Valkey または Redis OSS) で自動バックアップが有効になっているかどうかを確認します。自動バックアップが有効になっていない場合、またはクラスターの SnapshotRetentionLimit が指定された より小さい場合、ルールは NON_COMPLIANT ですsnapshotRetentionPeriod。

識別子： ELASTICACHE_AUTOMATIC_BACKUP_CHECK_ENABLED

リソースタイプ: AWS::ElastiCache::CacheCluster

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

snapshotRetentionPeriod (オプション), タイプ: int

> Valkey または Redis OSS の最小スナップショット保持期間。有効な値は 1 ~ 35 です。デフォルト値は 1 です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache-auto-minor-version-upgrade-check

Amazon ElastiCache クラスターで自動マイナーバージョンアップグレードが有効になっているかどうかを確認します。Redis または Valkey エンジンを使用していて、AutoMinorVersionUpgrade」が「true」に設定されていない場合、ElastiCache クラスターのルールは NON_COMPLIANT です。

識別子: ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

リソースタイプ: AWS::ElastiCache::CacheCluster

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache-rbac-auth-enabled

Amazon ElastiCache レプリケーショングループで RBAC 認証が有効になっているかどうかを確認します。Redis のバージョンが 6 以上で、「UserGroupIds」がない、空、または「`allowedUserGroupIDs`」パラメータで指定されたエントリと一致しない場合、このルールは NON_COMPLIANT になります。

識別子: ELASTICACHE_RBAC_AUTH_ENABLED

リソースタイプ: AWS::ElastiCache::ReplicationGroup

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

allowedUserGroupIDs (オプション), タイプ: CSV

ElastiCache レプリケーションアクセスに対して承認されたユーザーグループ ID のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache-redis-cluster-automatic-backup-check

Amazon ElastiCache Redis クラスターで自動バックアップが有効になっているかどうかを確認します。Redis クラスターの SnapshotRetentionLimit がSnapshotRetentionPeriod パラメータより小さい場合、ルールは NON_COMPLIANT です。例えば、パラメータが 15 の場合、snapshotRetentionPeriod が 0 ~ 15 であれば、ルールは準拠していません。

識別子: ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

リソースタイプ: AWS::ElastiCache::CacheCluster、AWS::ElastiCache::ReplicationGroup

トリガータイプ: 定期的

AWS リージョン : アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

snapshotRetentionPeriod (オプション), タイプ: int, デフォルト: 15

Redis クラスターの最小スナップショットの保持期間 (日数)。デフォルトは 15 日です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache-repl-grp-auto-failover-enabled

Amazon ElastiCache Redis レプリケーショングループで自動フェイルオーバーが有効になっているかどうかを確認します。‘AutomaticFailover’が‘enabled’に設定されていない場合、ElastiCache レプリケーショングループのルールは NON_COMPLIANT になります。

識別子: ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

リソースタイプ: AWS::ElastiCache::ReplicationGroup

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache-repl-grp-encrypted-at-rest

Amazon ElastiCache レプリケーショングループで encryption-at-rest が有効になっているかどうかをチェックします。'AtRestEncryptionEnabled' が無効になっている場合、または KMS キー ARN が approvedKMSKeyArns パラメータと一致しない場合、ElastiCache レプリケーショングループのルールは NON_COMPLIANT になります。

識別子: ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

リソースタイプ: AWS::ElastiCache::ReplicationGroup

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

approvedKMSKeyIds (オプション), タイプ: CSV

ElastiCache の使用に承認された KMS キー ID のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache-repl-grp-encrypted-in-transit

Amazon ElastiCache レプリケーショングループで encryption-in-transit が有効になっているかどうかをチェックします。‘TransitEncryptionEnabled’が‘false’に設定されていない場合、ElastiCache レプリケーショングループのルールは NON_COMPLIANT になります。

識別子: ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

リソースタイプ: AWS::ElastiCache::ReplicationGroup

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache-repl-grp-redis-auth-enabled

Amazon ElastiCacheレプリケーショングループで Redis AUTH が有効になっているかどうかを確認します。ElastiCache レプリケーショングループのノードの Redis バージョンが 6 未満で (バージョン 6 以上では Redis ACL を使用)、‘AuthToken’がないか、空/null の場合、ElastiCache レプリケーショングループのルールは NON_COMPLIANT となります。

識別子: ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

リソースタイプ: AWS::ElastiCache::ReplicationGroup

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべてのリージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache-subnet-group-check

Amazon ElastiCache クラスターがカスタムサブネットグループで設定されているかどうかを確認します。ElastiCache クラスターがデフォルトのサブネットグループを使用している場合、ルールは NON_COMPLIANT になります。

識別子: ELASTICACHE_SUBNET_GROUP_CHECK

リソースタイプ: AWS::ElastiCache::CacheCluster

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticache-supported-engine-version

ElastiCache クラスターが推奨エンジンバージョンと同じかそれ以降のバージョンを実行しているかどうかを確認します。ElastiCache クラスターの「Engine Vertion」が、指定されたエンジンの推奨バージョン未満の場合、ルールは NON_COMPLIANT になります。

識別子: ELASTICACHE_SUPPORTED_ENGINE_VERSION

リソースタイプ: AWS::ElastiCache::CacheCluster

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

latestMemcachedVersion, タイプ: 文字列

Memcached の最新の推奨エンジンバージョンです。有効な値はセマンティックバージョニング (SemVer) 形式で、メジャーバージョン、マイナーバージョン、およびパッチバージョン (例: 1.6 ではなく 1.6.6) に 3 成分数が付けられます。

latestRedisVersion, タイプ: 文字列

Redis の最新の推奨エンジンバージョンです。有効な値はセマンティックバージョニング (SemVer) 形式で、メジャーバージョン、マイナーバージョン、およびパッチバージョン (例: 7.0 ではなく 7.0.5) に 3 成分数が付けられます。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticbeanstalk-application-description

Elastic Beanstalk AWS アプリケーションに説明があるかどうかを確認します。configuration.description が存在しない場合、または空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： ELASTICBEANSTALK_APPLICATION_DESCRIPTION

リソースタイプ： AWS::ElasticBeanstalk::Application

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticbeanstalk-application-version-description

Elastic Beanstalk AWS アプリケーションバージョンに説明があるかどうかを確認します。configuration.description が存在しない場合、または空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： ELASTICBEANSTALK_APPLICATION_VERSION_DESCRIPTION

リソースタイプ： AWS::ElasticBeanstalk::ApplicationVersion

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticbeanstalk-environment-description

Elastic Beanstalk AWS 環境の説明があるかどうかを確認します。configuration.description が存在しない場合、または空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： ELASTICBEANSTALK_ENVIRONMENT_DESCRIPTION

リソースタイプ: AWS::ElasticBeanstalk::Environment

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticsearch-encrypted-at-rest

Amazon OpenSearch Service (以前は Elasticsearch と呼ばれていた) ドメインで保管時の暗号化設定が有効になっているかどうかを確認します。EncryptionAtRestOptions フィールドが有効でない場合、ルールは NON_COMPLIANT です。

Identifier: ELASTICSEARCH_ENCRYPTED_AT_REST

リソースタイプ: AWS::Elasticsearch::Domain

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticsearch-in-vpc-only

Amazon OpenSearch Service (以前は Elasticsearch と呼ばれていた) ドメインが Amazon Virtual Private Cloud (Amazon VPC) にあるかどうかを確認します。OpenSearch Service ドメインのエンドポイントがパブリックである場合、ルールは NON_COMPLIANT になります。

Identifier: ELASTICSEARCH_IN_VPC_ONLY

リソースタイプ: AWS::Elasticsearch::Domain

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elasticsearch-logs-to-cloudwatch

Amazon OpenSearch Service ドメインが、Amazon CloudWatch Logs にログを送信するように設定されているかどうかを確認します。Amazon ES ドメインに対してログが有効になっている場合、ルールは COMPLIANT です。ログ記録が設定されていない場合、このルールは NON_COMPLIANT です。

識別子: ELASTICSEARCH_LOGS_TO_CLOUDWATCH

リソースタイプ: AWS::Elasticsearch::Domain

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

logTypes (オプション), タイプ: CSV

有効になっているログのカンマ区切りリスト。有効な値は 「search」、「index」、「error」です。

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
...
```

*発行するログのタイプに応じて、SEARCH_SLOW_LOGS、ES_APPLICATION_LOGS、INDEX_SLOW_LOGS、AUDIT_LOGS のうち 1 つ以上のキーを持つオブジェクト。各キーには有効な LogPublishingOption 値が必要です。

プロアクティブ評価の詳細については、「Evaluation Mode」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

elasticsearch-node-to-node-encryption-check

OpenSearch Service (以前は Elasticsearch と呼ばれていた) ノードがエンドツーエンドで暗号化されているかどうかを確認します。ノード間の暗号化がドメイン上で有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

リソースタイプ: AWS::Elasticsearch::Domain

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

elastic-beanstalk-logs-to-cloudwatch

Elastic Beanstalk 環境が Amazon CloudWatch Logs AWS にログを送信するように設定されているかどうかを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

識別子: ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

リソースタイプ: AWS::ElasticBeanstalk::Environment

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

RetentionInDays (オプション), タイプ: 文字列

ログイベントが期限切れになるまでの日数を確認します。有効な値は 1、3、5、7、14、30、60、90、120、150、180、365、400、545、731、1827、3653 です。「logs.RetentionInDays」の値がこのパラメータと一致しない場合、ルールは NON_COMPLIANT です。

DeleteOnTerminate (オプション), タイプ: 文字列

環境終了時にログが削除されるように設定されているかどうかを確認します。有効な値は、「true」または「false」です。「logs.DeleteOnTerminate」の値がこのパラメータと一致しない場合、ルールは NON_COMPLIANT です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elastic-beanstalk-managed-updates-enabled

AWS Elastic Beanstalk 環境でマネージドプラットフォームの更新が有効になっているかどうかを確認します。`ManagedActionsEnabled` の値が true に設定されている場合、ルールは COMPLIANT です。`ManagedActionsEnabled` の値が false に設定されている場合、またはパラメータが指定されているもののその値が既存の設定と一致しない場合、ルールは NON_COMPLIANT です。

識別子: ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

リソースタイプ: AWS::ElasticBeanstalk::Environment

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

UpdateLevel (オプション), 型: 文字列

更新レベルが「minor」バージョン更新または「patch」バージョン更新に設定されているかどうかを示します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elbv2-acm-certificate-required

Application Load Balancer と Network Load Balancer に、 AWS Certificate Manager (ACM) の証明書を使用するように設定されたリスナーがあるかどうかを確認します。少なくとも 1 つのロードバランサーに、ACM からの証明書を使用しないよう設定されている、または ACM 証明書とは異なる証明書を使用して設定されているリスナーが少なくとも 1 つある場合、このルールは NON_COMPLIANT です。

識別子: ELBV2_ACM_CERTIFICATE_REQUIRED

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台

北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

AcmCertificatesAllowed (オプション), タイプ: CSV

証明書の Amazon リソースネーム (ARN) のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elbv2-listener-encryption-in-transit

ロードバランサーのリスナーが HTTPS または TLS 終了で設定されているかどうかを確認します。リスナーに HTTPS または TLS 終了が設定されていない場合、ルールは NON_COMPLIANT です。

識別子： ELBV2_LISTENER_ENCRYPTION_IN_TRANSIT

リソースタイプ： AWS::ElasticLoadBalancingV2::Listener

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (ソウル) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elbv2-multiple-az

Elastic ロードバランサー V2 (アプリケーション、ネットワーク、またはゲートウェイロードバランサー) が複数のアベイラビリティーゾーン (AZ) にマッピングされているかどうかを確認します。Elastic ロードバランサー V2 が 2 未満の AZ にマッピングされている場合、ルールは NON_COMPLIANT です。詳細については、「Application Load Balancer のアベイラビリティーゾーン」を参照してください。

識別子: ELBV2_MULTIPLE_AZ

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

minAvailabilityZones (オプション), タイプ: int

予想される AZ の最小数 (2 から 10 までの間)。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

elbv2-predefined-security-policy-ssl-check

Application Load Balancer (ALBs) または Network Load Balancer (NLBs) のリスナーが特定のセキュリティポリシーを使用しているかどうかを確認します。ALB の HTTPS リスナーまたは NLB の TLS リスナーが、指定したセキュリティポリシーを使用しない場合、ルールは NON_COMPLIANT です。

識別子： ELBV2_PREDEFINED_SECURITY_POLICY_SSL_CHECK

リソースタイプ： AWS::ElasticLoadBalancingV2::Listener

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

sslPolicies, タイプ: CSV

チェックするルールの SSL セキュリティポリシーのカンマ区切りリスト。たとえば、「ELBSecurityPolicy-TLS13-1-2-2021-06」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elb-acm-certificate-required

Classic Load Balancer が が提供する SSL 証明書を使用しているかどうかを確認します AWS Certificate Manager。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

識別子: ELB_ACM_CERTIFICATE_REQUIRED

リソースタイプ: AWS::ElasticLoadBalancing::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アフリカ (ケープタウン) 、アジアパシフィック (大阪) 、欧州 (ミラノ) 、イスラエル (テルアビブ) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elb-cross-zone-load-balancing-enabled

クロスゾーンロードバランシングが Classic Load Balancer に対して有効になっているかどうかを確認します。クロスゾーンロードバランシングが Classic Load Balancer に対して有効でない場合、ルールは NON_COMPLIANT になります。

識別子: ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

リソースタイプ: AWS::ElasticLoadBalancing::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elb-custom-security-policy-ssl-check

Classic Load Balancer の SSL リスナーがカスタムポリシーを使用しているかどうか確認します。このルールは、Classic Load Balancer の SSL リスナーがある場合のみ適用されます。

識別子: ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

リソースタイプ: AWS::ElasticLoadBalancing::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ジャカルタ) 、アジアパシフィック (大阪) 、アジアパシフィック (メルボルン) 、アジアパシフィック (台北) AWS を除く、サポートされているすべてのリージョン

パラメータ :

sslProtocolsAndCiphers, 型: 文字列

暗号とプロトコルのカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elb-deletion-protection-enabled

Elastic Load Balancer で削除保護が有効になっているかどうかを確認します。deletion_protection.enabled が false の場合、ルールは NON_COMPLIANT です。

識別子: ELB_DELETION_PROTECTION_ENABLED

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (大阪) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elb-logging-enabled

Application Load Balancer と Classic Load Balancer でログ記録が有効になっているかどうかを確認します。`access_logs.s3.enabled` が false で、`access_logs.S3.bucket` が入力した s3BucketName と同じでない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> このルールは、Network Load Balancer または ゲートウェイロードバランサーに適用されません。

識別子: ELB_LOGGING_ENABLED

リソースタイプ: AWS::ElasticLoadBalancing::LoadBalancer、AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

s3BucketNames (オプション), タイプ: CSV

Amazon ELB のログファイルを配信するための Amazon S3 バケット名のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elb-predefined-security-policy-ssl-check

Classic Load Balancer の SSL リスナーが事前定義済みポリシーを使用しているかどうか確認します。Classic Load Balancer の HTTPS/SSL リスナーのポリシーがパラメータ「`predefinedPolicyName`」の値と一致しない場合、ルールは NON_COMPLIANT です。

識別子: ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

リソースタイプ: AWS::ElasticLoadBalancing::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (大阪) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

predefinedPolicyName, 型: 文字列

事前定義済みポリシーの名前。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

elb-tls-https-listeners-only

Classic Load Balancer が SSL または HTTPS リスナーで設定されているかどうかを確認します。リスナーが SSL または HTTPS で設定されていない場合、ルールは NON_COMPLIANT です。

- Classic Load Balancer にリスナーが設定されていない場合、ルールは を返しますNOT_APPLICABLE。
- Classic Load Balancer のリスナーが SSL または HTTPS で設定されている場合、ルールは COMPLIANT です。
- リスナーが SSL または HTTPS で設定されていない場合、ルールは NON_COMPLIANT です。

識別子: ELB_TLS_HTTPS_LISTENERS_ONLY

リソースタイプ: AWS::ElasticLoadBalancing::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： 中東 (アラブ首長国連邦) 、アジアパシフィック (大阪) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

emr-block-public-access

Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっているかどうかを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。

識別子: EMR_BLOCK_PUBLIC_ACCESS

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

emr-kerberos-enabled

Amazon EMR クラスターで Kerberos が有効になっていることを確認します。セキュリティ構成がクラスターにアタッチされていない場合、またはセキュリティ構成が指定されたルールパラメータを満たしていない場合、ルールは NON_COMPLIANT です。

識別子: EMR_KERBEROS_ENABLED

リソースタイプ: AWS::EMR::Cluster

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

TicketLifetimeInHours (オプション), タイプ: int

クラスターの KDC によって発行された Kerberos チケットが有効な期間。

Realm (オプション), 型: 文字列

信頼関係の他の領域の Kerberos 領域名。

Domain (オプション), 型: 文字列

信頼関係の他の領域のドメイン名。

AdminServer (オプション), 型: 文字列

信頼関係の他の領域の管理サーバーの完全修飾ドメイン。

KdcServer (オプション), 型: 文字列

信頼関係の他の領域の KDC サーバーの完全修飾ドメイン。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

emr-master-no-public-ip

Amazon EMR クラスターのプライマリノードにパブリック IP があるかどうかを確認します。プライマリノードにパブリック IP がある場合、ルールは NON_COMPLIANT です。

> **Note**
>
> このルールは、RUNNING または WAITING 状態のクラスターを確認します。このルールでは、正確な評価を行うために `AWS::EC2::Instance` リソースタイプの設定を有効化する必要があります。

識別子: EMR_MASTER_NO_PUBLIC_IP

リソースタイプ: AWS::EMR::Cluster、AWS::EC2::Instance

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (大阪) 、アジアパシフィック (メルボルン) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

emr-security-configuration-encryption-rest

Amazon EMR セキュリティ設定で保管時の暗号化が有効になっているかどうかを確認します。configuration.SecurityConfiguration.EncryptionConfiguration.EnableAtRestEncryption が false の場合、ルールは NON_COMPLIANT です。

識別子： EMR_SECURITY_CONFIGURATION_ENCRYPTION_REST

リソースタイプ： AWS::EMR::SecurityConfiguration

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

emr-security-configuration-encryption-transit

Amazon EMR セキュリティ設定で転送中の暗号化が有効になっているかどうかを確認します。configuration.SecurityConfiguration.EncryptionConfiguration.EnableInTransitEncryption が false の場合、ルールは NON_COMPLIANT です。

識別子： EMR_SECURITY_CONFIGURATION_ENCRYPTION_TRANSIT

リソースタイプ： AWS::EMR::SecurityConfiguration

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

encrypted-volumes

アタッチされた Amazon EBS ボリュームが暗号化されているか、オプションで指定された KMS キーで暗号化されているかを確認します。アタッチされた EBS ボリュームが暗号化されていな

いか、指定されたパラメータに含まれていない KMS キーで暗号化されている場合、ルールは NON_COMPLIANT になります。

識別子: ENCRYPTED_VOLUMES

リソースタイプ: AWS::EC2::Volume

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

kmsId (オプション), 型: 文字列

ボリュームの暗号化に使用する KMS キーの ID または ARN。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

event-data-store-cmk-encryption-enabled

AWS Cloud Trail イベントデータストアでカスタマーマネージド KMS AWS キーが有効になっているかどうかを確認します。イベントデータストアでカスタマーマネージド KMS キーが無効になっている場合、ルールは NON_COMPLIANT です。必要に応じて、チェックするルールの KMS キーのリストを指定できます。

識別子： EVENT_DATA_STORE_CMK_ENCRYPTION_ENABLED

リソースタイプ： AWS::CloudTrail::EventDataStore

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

kmsKeyArns (オプション), タイプ: CSV

チェックするルールの KMS AWS キーの Amazon リソースネーム (ARNs) のカンマ区切りリスト。指定した場合、 AWS Cloud Trail イベントデータストアがこれらの KMS キーのいずれかで暗号化されていない場合、ルールは NON_COMPLIANT です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

evidently-launch-description

Amazon CloudWatch Evidently の起動に説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： EVIDENTLY_LAUNCH_DESCRIPTION

リソースタイプ： AWS::Evidently::Launch

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

evidently-launch-tagged

Amazon CloudWatch Evidently 起動にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EVIDENTLY_LAUNCH_TAGGED

リソースタイプ： AWS::Evidently::Launch

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

evidently-project-description

Amazon CloudWatch Evidently プロジェクトに説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： EVIDENTLY_PROJECT_DESCRIPTION

リソースタイプ： AWS::Evidently::Project

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

evidently-project-tagged

Amazon CloudWatch Evidently プロジェクトにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EVIDENTLY_PROJECT_TAGGED

リソースタイプ： AWS::Evidently::Project

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

evidently-segment-description

Amazon CloudWatch Evidently セグメントに説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： EVIDENTLY_SEGMENT_DESCRIPTION

リソースタイプ： AWS::Evidently::Segment

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

evidently-segment-tagged

Amazon CloudWatch Evidently セグメントにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： EVIDENTLY_SEGMENT_TAGGED

リソースタイプ： AWS::Evidently::Segment

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fis-experiment-template-log-configuration-exists

FIS 実験テンプレート AWS に実験ログが設定されているかどうかを確認します。configuration.LogConfiguration が存在しない場合、ルールは NON_COMPLIANT です。

識別子： FIS_EXPERIMENT_TEMPLATE_LOG_CONFIGURATION_EXISTS

リソースタイプ： AWS::FIS::ExperimentTemplate

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fis-experiment-template-tagged

FIS AWS 実験テンプレートにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： FIS_EXPERIMENT_TEMPLATE_TAGGED

リソースタイプ： AWS::FIS::ExperimentTemplate

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fms-shield-resource-policy-check

Shield Advanced が保護できるリソースが AWS Shield Advanced によって保護されているかどうかを確認します。指定されたリソースが保護されていない場合、ルールは NON_COMPLIANT です。

識別子: FMS_SHIELD_RESOURCE_POLICY_CHECK

リソースタイプ: AWS::CloudFront::Distribution、AWS::ElasticLoadBalancingV2::LoadBalancer、AWS::WAFRegional::WebA

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

webACLId, タイプ: 文字列

ウェブ ACL の一意の識別子。

resourceTypes, タイプ: 文字列

チェックするルールに指定するリソースタイプ。

resourceTags (オプション), タイプ: 文字列

チェックするルールに指定するリソースタグ。たとえば、{ "tagKey1" : ["tagValue1"]、"tagKey2" : ["tagValue2"、"tagValue3"] } です。

excludeResourceTags (オプション), タイプ：ブール値

true の場合、ルールは resourceTags で指定されたリソースを除外します。false の場合、ルールには resourceTags で指定されたすべてのリソースが含まれます。

fmsManagedToken (オプション), タイプ: 文字列

アカウントでルールを作成するときに AWS Firewall Manager によって生成されたトークン。AWS Config は、このルールを作成するときにこのパラメータを無視します。

fmsRemediationEnabled (オプション), タイプ：ブール値

true の場合、 AWS Firewall Manager は FMS policy. AWS Config に従って NON_COMPLIANT リソースを更新します。このルールを作成すると、このパラメータは無視されます。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fms-webacl-resource-policy-check

ウェブ ACL が、Application Load Balancer、API Gateway ステージ、または Amazon CloudFront ディストリビューションに関連付けられているかどうかを確認します。がこのルール AWS Firewall Manager を作成すると、FMS ポリシー所有者は FMS ポリシー`WebACLId`で を指定し、オプションで修復を有効にできます。

識別子: FMS_WEBACL_RESOURCE_POLICY_CHECK

リソースタイプ: AWS::CloudFront::Distribution、AWS::ApiGateway::Stage、AWS::ElasticLoadBalancingV2::LoadBalancer、

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

webACLId, 型: 文字列

ウェブ ACL の WebACLId。

resourceTags (オプション), 型: 文字列

ルールが関連付けるべきリソースタグ (ApplicationLoadBalancer、ApiGatewayStage、および CloudFront ディストリビューション)。(例: {"tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] })

excludeResourceTags (オプション), 型: ブール値

true の場合、resourceTags に一致するリソースを除外します。

fmsManagedToken (オプション), タイプ: 文字列

お客様のアカウントでルールを作成するときに AWS Firewall Manager によって生成されたトークン。 AWS Config は、お客様がこのルールを作成するときにこのパラメータを無視します。

fmsRemediationEnabled (オプション), タイプ：ブール値

true の場合、 AWS Firewall Manager は FMS ポリシーに従って非準拠のリソースを更新します。 AWS Config は、お客様がこのルールを作成するときにこのパラメータを無視します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fms-webacl-rulegroup-association-check

ウェブ ACL に関連付けるルールグループに適切な優先順位が付けられていることを確認します。適切な優先度は、ruleGroups パラメータのルールグループのランクによって決定されます。がこのルール AWS Firewall Manager を作成すると、優先度が最も高い 0 の後に 1、2 などが割り当てられます。FMS ポリシー所有者は FMS ポリシーで `ruleGroups` ランクを指定し、必要に応じて修復を有効にできます。

識別子: FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

リソースタイプ: AWS::WAF::WebACL、AWS::WAFRegional::WebACL

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

ruleGroups, 型: 文字列

RuleGroupIds と WafOverrideAction のペアのカンマ区切りのリスト。(例: ruleGroupId-1:NONE, ruleGroupId2:COUNT)

fmsManagedToken (オプション), タイプ: 文字列

お客様のアカウントでルールを作成するときに AWS Firewall Manager によって生成されたトークン。 AWS Config は、お客様がこのルールを作成するときにこのパラメータを無視します。

fmsRemediationEnabled (オプション), タイプ：ブール値

true の場合、 AWS Firewall Manager は FMS ポリシーに従って非準拠のリソースを更新します。AWS Config は、お客様がこのルールを作成するときにこのパラメータを無視します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

frauddetector-entity-type-tagged

Amazon Fraud Detector エンティティタイプにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： FRAUDDETECTOR_ENTITY_TYPE_TAGGED

リソースタイプ： AWS::FraudDetector::EntityType

トリガータイプ: 設定変更

AWS リージョン： 米国東部 (オハイオ) 、欧州 (アイルランド) 、米国東部 (バージニア北部) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

frauddetector-label-tagged

Amazon Fraud Detector ラベルにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： FRAUDDETECTOR_LABEL_TAGGED

リソースタイプ： AWS::FraudDetector::Label

トリガータイプ: 設定変更

AWS リージョン： 米国東部 (オハイオ) 、欧州 (アイルランド) 、米国東部 (バージニア北部) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

frauddetector-outcome-tagged

Amazon Fraud Detector の結果にタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： FRAUDDETECTOR_OUTCOME_TAGGED

リソースタイプ： AWS::FraudDetector::Outcome

トリガータイプ: 設定変更

AWS リージョン： 米国東部 (オハイオ) 、欧州 (アイルランド) 、米国東部 (バージニア北部) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

frauddetector-variable-tagged

Amazon Fraud Detector 変数にタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： FRAUDDETECTOR_VARIABLE_TAGGED

リソースタイプ： AWS::FraudDetector::Variable

トリガータイプ: 設定変更

AWS リージョン： 米国東部 (オハイオ) 、欧州 (アイルランド) 、米国東部 (バージニア北部) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fsx-last-backup-recovery-point-created

Amazon FSx ファイルシステムのリカバリポイントが作成されたかどうかを確認します。Amazon FSx ファイルシステムに対応するリカバリポイントが指定した期間内に作成されていない場合、ルールは NON_COMPLIANT です。

識別子: FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::FSx::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon FSx ファイルシステムのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)

resourceId (オプション), 型: 文字列

チェックするルールの Amazon FSx ファイルシステムの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fsx-lustre-copy-tags-to-backups

Amazon FSx for Lustre ファイルシステムがタグをバックアップにコピーするように設定されているかどうかを確認します。Lustre ファイルシステムがタグをバックアップにコピーするように設定されていない場合、ルールは NON_COMPLIANT です。

識別子: FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

リソースタイプ: AWS::FSx::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fsx-meets-restore-time-target

Amazon FSx ファイルシステムの復元時間が、指定された期間と一致しているかどうかを確認します。Amazon FSx ファイルシステムの LatestRestoreExecutionTimeMinutes が maxRestoreTime の値より大きい場合、ルールは NON_COMPLIANT です。

識別子: FSX_MEETS_RESTORE_TIME_TARGET

リソースタイプ: AWS::FSx::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各 AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

maxRestoreTime, タイプ: int

最大許容復元ランタイムの数値。

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon FSx ファイルシステムのタグ (JSON 形式)

resourceId (オプション), 型: 文字列

チェックするルールの Amazon FSx ファイルシステムの ID。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fsx-ontap-deployment-type-check

Amazon FSx for NetApp ONTAP ファイルシステムが特定のデプロイタイプで設定されているかどうかを確認します。Amazon FSx for NetApp ONTAP ファイルシステムが指定したデプロイタイプで設定されていない場合、ルールは NON_COMPLIANT です。

識別子： FSX_ONTAP_DEPLOYMENT_TYPE_CHECK

リソースタイプ: AWS::FSx::FileSystem

トリガータイプ: 定期的

AWS リージョン： AWS 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) を除く、サポートされているすべての リージョン

パラメータ :

deploymentTypes, タイプ: CSV

チェックするルールで許可されるデプロイタイプのカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fsx-openzfs-copy-tags-enabled

Amazon FSx for OpenZFS ファイルシステムがタグをバックアップとボリュームにコピーするように設定されているかどうかを確認します。FSx for OpenZFS ファイルシステムがタグをバックアップとボリュームにコピーするように設定されていない場合、ルールは NON_COMPLIANT です。

識別子: FSX_OPENZFS_COPY_TAGS_ENABLED

リソースタイプ: AWS::FSx::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fsx-openzfs-deployment-type-check

Amazon FSx for OpenZFS ファイルシステムが特定のデプロイタイプで設定されているかどうかを確認します。FSx for OpenZFS ファイルシステムが指定したデプロイタイプで設定されていない場合、ルールは NON_COMPLIANT です。

識別子： FSX_OPENZFS_DEPLOYMENT_TYPE_CHECK

リソースタイプ: AWS::FSx::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

deploymentTypes, タイプ: CSV

チェックするルールで許可されるデプロイタイプのカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fsx-resources-protected-by-backup-plan

Amazon FSx ファイルシステムがバックアップ計画で保護されているかどうかを確認します。Amazon FSx ファイルがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

識別子:FSX_RESOURCES_PROTECTED_BACKUP_PLAN

リソースタイプ: AWS::FSx::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon FSx ファイルシステムのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)

resourceId (オプション), 型: 文字列

ルールをチェックする Amazon FSx ファイルシステムの ID

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fsx-windows-audit-log-configured

Amazon FSx for Windows File Server ファイルシステムで、ファイルアクセス監査が有効になっているかどうかを確認します。FSx for Windows File Server ファイルシステムで、ファイルアクセス監査が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: FSX_WINDOWS_AUDIT_LOG_CONFIGURED

リソースタイプ: AWS::FSx::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

fsx-windows-deployment-type-check

Amazon FSx for WINDOWS ファイルシステムが特定のデプロイタイプで設定されているかどうかを確認します。FSx for WINDOWS ファイルシステムが指定したデプロイタイプで設定されていない場合、ルールは NON_COMPLIANT です。

識別子： FSX_WINDOWS_DEPLOYMENT_TYPE_CHECK

リソースタイプ: AWS::FSx::FileSystem

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、欧州 (パリ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

deploymentTypes, タイプ: CSV

チェックするルールで許可されるデプロイタイプのカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

glb-listener-tagged

Gateway Load Balancer リスナーにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： GLB_LISTENER_TAGGED

リソースタイプ： AWS::ElasticLoadBalancingV2::Listener

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

global-endpoint-event-replication-enabled

Amazon EventBridge グローバルエンドポイントでイベントレプリケーションが有効になっているかどうかを確認します。イベントのレプリケーションが有効でない場合、ルールは NON_COMPLIANT です。

識別子: GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

リソースタイプ: AWS::Events::Endpoint

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (大阪) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

glue-job-logging-enabled

Glue AWS ジョブでログ記録が有効になっているかどうかを確認します。Glue ジョブで Amazon CloudWatch AWS ログが有効になっていない場合、ルールは NON_COMPLIANT です。 Amazon CloudWatch logs

識別子: GLUE_JOB_LOGGING_ENABLED

リソースタイプ： AWS::Glue::Job

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

glue-ml-transform-encrypted-at-rest

AWS Glue ML 変換で保管時の暗号化が有効になっているかどうかを確認します。MLUserDataEncryptionMode が DISABLED に設定されている場合、ルールは NON_COMPLIANT です。

識別子: GLUE_ML_TRANSFORM_ENCRYPTED_AT_REST

リソースタイプ: AWS::Glue::MLTransform

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

glue-spark-job-supported-version

指定されたサポートされている最小 AWS Glue バージョンで Glue Spark AWS ジョブが実行されているかどうかを確認します。Glue Spark ジョブが、指定したサポートされている最小 AWS Glue バージョンで実行されていない場合、ルールは NON_COMPLIANT AWS です。

識別子： GLUE_SPARK_JOB_SUPPORTED_VERSION

リソースタイプ： AWS::Glue::Job

トリガータイプ: 設定変更

AWS リージョン： AWS 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) を除く、サポートされているすべての リージョン

パラメータ：

minimumSupportedGlueVersion, タイプ: 文字列

ルールがチェックするには、サポートされている最小 Glue AWS バージョンを指定する必要があります。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-ec2-protection-runtime-enabled

自動エージェント管理による ECS Runtime Monitoring が Amazon GuardDuty ディテクターで有効になっているかどうかを確認します。アカウントまたは組織内の少なくとも 1 つのメンバーアカウントでこの機能が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子： GUARDDUTY_EC2_PROTECTION_RUNTIME_ENABLED

リソースタイプ: AWS::GuardDuty::Detector

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-ecs-protection-runtime-enabled

自動エージェント管理による ECS Runtime Monitoring が Amazon GuardDuty ディテクターで有効になっているかどうかを確認します。アカウントまたは組織内の少なくとも 1 つのメンバーアカウントでこの機能が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子： GUARDDUTY_ECS_PROTECTION_RUNTIME_ENABLED

リソースタイプ: AWS::GuardDuty::Detector

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-eks-protection-audit-enabled

Amazon Elastic Kubernetes Service (Amazon EKS) の監査ログモニタリングが、アカウントの Amazon GuardDuty ディテクターに対して有効になっているかどうかを確認します。アカウントで EKS 監査ログモニタリング機能が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: GUARDDUTY_EKS_PROTECTION_AUDIT_ENABLED

リソースタイプ: AWS::GuardDuty::Detector

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-eks-protection-runtime-enabled

アカウントの GuardDuty ディテクターで、自動エージェント管理による Amazon EKS Runtime Monitoring が有効になっているかどうかを確認します。GuardDuty の自動エージェント管理による EKS Runtime Monitoring がアカウントで有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: GUARDDUTY_EKS_PROTECTION_RUNTIME_ENABLED

リソースタイプ: AWS::GuardDuty::Detector

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィッ

ク (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-enabled-centralized

AWS アカウントと AWS リージョンで Amazon GuardDuty が有効になっているかどうかを確認します。一元化のために AWS アカウントを指定すると、ルールは一元化されたアカウントで GuardDuty の結果を評価します。GuardDuty が有効になっている場合、ルールは COMPLIANT です。

識別子: GUARDDUTY_ENABLED_CENTRALIZED

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

CentralMonitoringAccount (オプション), タイプ: 文字列

Amazon GuardDuty の結果を一元化できる AWS アカウント (12 桁) のカンマ区切りリスト。Amazon GuardDuty

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-lambda-protection-enabled

アカウントの Amazon GuardDuty ディテクターで Lambda Protection が有効になっているかどうかを確認します。Amazon GuardDuty の Lambda Protection 機能がアカウントで有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: GUARDDUTY_LAMBDA_PROTECTION_ENABLED

リソースタイプ: AWS::GuardDuty::Detector

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-malware-protection-enabled

アカウントの Amazon GuardDuty ディテクターで Malware Protection が有効になっているかどうかを確認します。Amazon GuardDuty の Malware Protection 機能がアカウントで有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: GUARDDUTY_MALWARE_PROTECTION_ENABLED

リソースタイプ: AWS::GuardDuty::Detector

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシ

フィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-non-archived-findings

Amazon GuardDuty にアーカイブされていない検出結果があるかどうかを確認します。GuardDuty に、daysLowSev/daysMediumSev/`daysHighSev` パラメータで指定されている値よりも古い、重要度が低/中/高のアーカイブされていない検出結果がある場合、ルールは NON_COMPLIANT です。

識別子: GUARDDUTY_NON_ARCHIVED_FINDINGS

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

daysLowSev (オプション), タイプ: int, デフォルト: 30

Amazon GuardDuty の低重大度の結果をアーカイブしないまま保持できる日数。デフォルトは 30 日間です。

daysMediumSev (オプション), タイプ: int, デフォルト: 7

Amazon GuardDuty の重要度が中の検出結果をアーカイブしないまま保持できる日数。デフォルトは 7 日間です。

daysHighSev (オプション), タイプ: int, デフォルト: 1

Amazon GuardDuty の高重大度の結果をアーカイブしないまま保持できる日数。デフォルトは 1 日です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-rds-protection-enabled

アカウントの Amazon GuardDuty ディテクターに対して Amazon Relational Database Service (Amazon RDS) 保護が有効になっているかどうかを確認します。Amazon GuardDuty の Amazon RDS 保護機能がアカウントに対して有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: GUARDDUTY_RDS_PROTECTION_ENABLED

リソースタイプ: AWS::GuardDuty::Detector

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-runtime-monitoring-enabled

アカウントまたは組織の Amazon GuardDuty ディテクターで Runtime Monitoring が有効になっているかどうかを確認します。GuardDuty の Runtime Monitoring がアカウントまたは組織内の少なくとも 1 つのメンバーアカウントに対して有効になっていない場合、ルールは NON_COMPLIANT です。

識別子： GUARDDUTY_RUNTIME_MONITORING_ENABLED

リソースタイプ: AWS::GuardDuty::Detector

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

guardduty-s3-protection-enabled

アカウントの Amazon GuardDuty Detector で S3 Protection が有効になっているかどうかを確認します。Amazon GuardDuty の S3 保護機能がアカウントで有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: GUARDDUTY_S3_PROTECTION_ENABLED

リソースタイプ: AWS::GuardDuty::Detector

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-customer-policy-blocked-kms-actions

作成したマネージド AWS Identity and Access Management (IAM) ポリシーが、すべての KMS キーリソースでブロックされた KMS AWS アクションを許可していないかどうかを確認します。マネージド IAM ポリシーによってすべての KMS AWS キーでブロックされたアクションが許可されている場合、ルールは NON_COMPLIANT です。

> **Note**
>
> 非公開と見なされるには、IAM ポリシーが固定値へのアクセスのみを許可する必要があります。つまり、ワイルドカードまたは IAM ポリシー要素 Variables を含まない値です。

識別子: IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

リソースタイプ: AWS::IAM::Policy

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

blockedActionsPatterns, タイプ: CSV

チェックするルールのブロックされた KMS アクションパターンのカンマ区切りリスト。IAM カスタマー管理ポリシーで、指定したアクションのすべてのリソースへのワイルドカードアクセスが許可されている場合、ルールは NON_COMPLIANT です。

excludePermissionBoundaryPolicy (オプション), 型: ブール値

許可の境界として使用される IAM ポリシーの評価を除外するブールフラグ。「true」に設定すると、ルールで許可の境界は評価に含まれません。それ以外の場合、値が「false」に設定されていると、スコープ内のすべての IAM ポリシーが評価されます。デフォルト値は「false」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-external-access-analyzer-enabled

外部アクセス用の IAM Access Analyzer がリージョンごとにアカウントでアクティブ化されているかどうかを確認します。リージョンに外部アクセス用のアナライザーがない場合、または「ステータス」属性が「アクティブ」に設定されていない場合、ルールは NON_COMPLIANT です。

識別子: IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各 AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-group-has-users-check

IAM グループに少なくとも 1 人の IAM ユーザーが存在するかどうか確認します。

識別子: IAM_GROUP_HAS_USERS_CHECK

リソースタイプ: AWS::IAM::Group

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-inline-policy-blocked-kms-actions

IAM ユーザー、ロール、グループにアタッチされたインラインポリシーが、すべての KMS AWS キーでブロックされたアクションを許可していないかどうかを確認します。インラインポリシー内のすべての KMS AWS キーでブロックされたアクションが許可されている場合、ルールは NON_COMPLIANT です。

識別子: IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

リソースタイプ: AWS::IAM::Group、AWS::IAM::Role、AWS::IAM::User

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、

メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

blockedActionsPatterns, タイプ: CSV

ブロックされている KMS アクションパターンのカンマ区切りリスト。(例: kms:*, kms:Decrypt, kms:ReEncrypt*)

excludeRoleByManagementAccount (オプション), 型: ブール値

組織管理アカウントによってのみ引き受けできるロールの場合は、そのロールを除外します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-no-inline-policy-check

インラインポリシー機能が使用されていないかどうかを確認します。 AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループにインラインポリシーがある場合、ルールは NON_COMPLIANT です。

識別子: IAM_NO_INLINE_POLICY_CHECK

リソースタイプ: AWS::IAM::User、AWS::IAM::Role、AWS::IAM::Group

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-oidc-provider-tagged

IAM OIDC AWS プロバイダーにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IAM_OIDC_PROVIDER_TAGGED

リソースタイプ： AWS::IAM::OIDCProvider

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-password-policy

AWS Identity and Access Management (IAM) ユーザーのアカウントパスワードポリシーが、パラメータに示されている指定された要件を満たしているかどうかを確認します。アカウントのパスワードポリシーが指定の要件を満たしていない場合、ルールは NON_COMPLIANT です。

> **Important**
>
> ルールのパラメータの `true` および `false` の値は、大文字と小文字が区別されます `true` が小文字で入力されていない場合、`false.` として扱われます。

> **Note**
>
> デフォルトの IAM パスワードポリシーの評価結果
> デフォルトの IAM パスワードポリシーが使用されている場合、このルールでは NON_COMPLIANT としてマークされます。
> マネージドルールとグローバル IAM リソースタイプ
> 2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および `AWS::IAM::User`) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降、 でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。
> 少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
> 不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

識別子: IAM_PASSWORD_POLICY

トリガータイプ: 定期的

AWS リージョン： イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS を除く、サポートされているすべての リージョン

パラメータ :

RequireUppercaseCharacters (オプション), 型: ブール値, デフォルト: true

パスワードには少なくとも 1 つの大文字が必要です。

RequireLowercaseCharacters (オプション), 型: ブール値, デフォルト: true

パスワードには少なくとも 1 つの小文字が必要です。

RequireSymbols (オプション), 型: ブール値, デフォルト: true

パスワードには少なくとも 1 つの記号が必要です。

RequireNumbers (オプション), 型: ブール値, デフォルト: true

パスワードには少なくとも 1 つの数字が必要です。

MinimumPasswordLength (オプション), タイプ: int, デフォルト: 14

パスワードの最小長。

PasswordReusePrevention (オプション), タイプ: int, デフォルト: 24

パスワードを再利用できるまでの他のパスワードの使用回数。

MaxPasswordAge (オプション), タイプ: int, デフォルト: 90

パスワードが有効期限切れになるまでの日数。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-policy-blacklisted-check

入力パラメータのポリシー Amazon リソースネーム (ARN) が IAM リソースにアタッチされているかどうか、各 AWS Identity and Access Management (IAM) リソースをチェックします。ポリシー ARN が IAM リソースにアタッチされている場合、ルールは NON_COMPLIANT です。

識別子: IAM_POLICY_BLACKLISTED_CHECK

リソースタイプ: AWS::IAM::User、AWS::IAM::Group、AWS::IAM::Role

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

policyArns, タイプ: CSV, Default: arn:aws:iam::aws:policy/AdministratorAccess

IAM エンティティにアタッチすべきではない IAM ポリシー arn のカンマ区切りリスト。

exceptionList (オプション), タイプ: CSV

リソースタイプのカンマ区切りリストとリソース名ペアのリスト。例: users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3]。

> **Note**
>
> 例外リストには、完全な ARN ではなく、リソースの名前を指定します。無効: `arn:aws:iam::444455556666:role/Admin`。有効: `Admin`。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-policy-in-use

IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされているかどうかを確認します。

> **Note**
>
> マネージドルールとグローバル IAM リソースタイプ
> 2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および

`AWS::IAM::User`) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降、 でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。
少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

識別子: IAM_POLICY_IN_USE

リソースタイプ: AWS::IAM::Policy

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

policyARN, 型: 文字列

チェック対象の IAM ポリシー ARN。

policyUsageType (オプション), 型: 文字列

ポリシーを IAM ユーザー、グループ、またはロールにアタッチするかどうかを指定します。有効な値は、IAM_USER、IAM_GROUP、IAM_ROLE、または ANY です。デフォルト値は ANY です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-policy-no-statements-with-admin-access

作成した AWS Identity and Access Management (IAM) ポリシーに、すべてのリソースに対するすべてのアクションにアクセス許可を付与する Allow ステートメントがあるかどうかを確認します。いずれかのカスタマー管理 IAM ポリシーステートメントに、"Resource": "*" に対して "Action": "*" が "Effect": "Allow" になっている場合、ルールは NON_COMPLIANT です。

> **Note**
>
> このルールは、カスタマー管理ポリシーのみを評価します。このルールは、インラインポリシーまたは AWS 管理ポリシーを評価しません。この違いに関する詳細については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシー」を参照してください。

次のポリシーは NON_COMPLIANT です。

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

次のポリシーは COMPLIANT です。

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

識別子: IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

リソースタイプ: AWS::IAM::Policy

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

excludePermissionBoundaryPolicy (オプション), 型: ブール値

許可の境界として使用される IAM ポリシーの評価を除外するブールフラグ。「true」に設定すると、ルールで許可の境界は評価に含まれません。それ以外の場合、値が「false」に設定されていると、スコープ内のすべての IAM ポリシーが評価されます。デフォルト値は「false」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-policy-no-statements-with-full-access

作成した AWS Identity and Access Management (IAM) ポリシーが、個々の AWS リソースに対するすべてのアクションにアクセス許可を付与しているかどうかを確認します。カスタマー管理 IAM ポリシーで少なくとも 1 つの AWS サービスへのフルアクセスが許可されている場合、ルールは NON_COMPLIANT です。

コンテキスト: 最小特権の原則に従って、 AWS サービスにアクセス許可を付与する場合は、IAM ポリシーで許可されているアクションを制限することをお勧めします。このアプローチは、必要なアクションを正確に指定して必要なアクセス許可のみを付与し、`ec2:*` などのサービスに無制限のワイルドカードを使用しないようにするのに役立ちます。

場合によっては、DescribeFlowLogs や DescribeAvailabilityZones など、同様のプレフィックスを持つ複数のアクションを許可する場合があります。これらのケースでは、共通プレフィクスにサフィッ

クス付きワイルドカード (例: `ec2:Describe*`) を追加することができます。関連するアクションをグループ化すると、IAM ポリシーのサイズ制限に達するのを防ぐことができます。

このルールは、サフィックス付きワイルドカード (例: `ec2:Describe*`) でプレフィックス付きアクションを使用する場合、COMPLIANT を返します。このルールは、無制限のワイルドカード (例: `ec2:*`) を使用する場合のみ NON_COMPLIANT を返します。

> **Note**
>
> このルールは、カスタマー管理ポリシーのみを評価します。このルールは、インラインポリシーまたは AWS 管理ポリシーを評価しません。この違いに関する詳細については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシー」を参照してください。

[Identifier] (識別子): IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

リソースタイプ: AWS::IAM::Policy

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

excludePermissionBoundaryPolicy (オプション), 型: ブール値

許可の境界として使用される IAM ポリシーの評価を除外するブールフラグ。「true」に設定すると、ルールで許可の境界は評価に含まれません。それ以外の場合、値が「false」に設定されていると、スコープ内のすべての IAM ポリシーが評価されます。デフォルト値は「false」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

iam-role-managed-policy-check

管理ポリシーのリストで指定されたすべての管理ポリシーが AWS Identity and Access Management (IAM) ロールにアタッチされているかどうかを確認します。IAM ロールに管理ポリシーがアタッチされていない場合、ルールは NON_COMPLIANT です。

識別子: IAM_ROLE_MANAGED_POLICY_CHECK

リソースタイプ: AWS::IAM::Role

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

managedPolicyArns, タイプ: CSV

> AWS マネージドポリシーのカンマ区切りリスト Amazon リソースネーム (ARNs)。詳細については、「IAM ユーザーガイド」の「Amazon リソースネーム (ARN)」および「AWS マネージドポリシー」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

iam-root-access-key-check

ルートユーザーアクセスキーがあるかどうかを確認します。ユーザーアクセスキーが存在しない場合、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。

> **Note**
>
> マネージドルールとグローバル IAM リソースタイプ

2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および `AWS::IAM::User`) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降、 でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。
少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

識別子: IAM_ROOT_ACCESS_KEY_CHECK

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

iam-saml-provider-tagged

IAM SAML AWS プロバイダーにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IAM_SAML_PROVIDER_TAGGED

リソースタイプ： AWS::IAM::SAMLProvider

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-server-certificate-expiration-check

IAM AWS に保存されている IAM SSL/TLS サーバー証明書の有効期限が切れているかどうかを確認します。IAM サーバー証明書の有効期限が切れている場合、ルールは NON_COMPLIANT です。

識別子: IAM_SERVER_CERTIFICATE_EXPIRATION_CHECK

リソースタイプ: AWS::IAM::ServerCertificate

トリガータイプ: 定期的

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-server-certificate-tagged

IAM サーバー証明書 AWS にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IAM_SERVER_CERTIFICATE_TAGGED

リソースタイプ: AWS::IAM::ServerCertificate

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-user-group-membership-check

IAM ユーザーが少なくとも 1 つの IAM グループのメンバーであるかどうかを確認します。

識別子: IAM_USER_GROUP_MEMBERSHIP_CHECK

リソースタイプ: AWS::IAM::User

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

groupNames (オプション), 型: 文字列

IAM ユーザーがメンバーである必要がある IAM グループのカンマ区切りリスト。

> **Note**
> このルールは、コンマを含むグループ名をサポートしていません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-user-mfa-enabled

AWS Identity and Access Management (IAM) ユーザーが多要素認証 (MFA) が有効になっているかどうかを確認します。少なくとも 1 人の IAM ユーザーに対して MFA が有効になっていない場合、ルールは NON_COMPLIANT です。

> **Note**
> マネージドルールとグローバル IAM リソースタイプ
> 2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および `AWS::IAM::User`) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS

Config 以降に でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。
少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

識別子: IAM_USER_MFA_ENABLED

リソースタイプ: AWS::IAM::User

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

iam-user-no-policies-check

AWS Identity and Access Management (IAM) ユーザーにポリシーがアタッチされていないかどうかを確認します。IAM ユーザーは、IAM グループまたはロールからアクセス許可を継承する

必要があります。IAM ユーザーにアタッチされているポリシーが最低 1 件ある場合、ルールは NON_COMPLIANT です。

識別子: IAM_USER_NO_POLICIES_CHECK

リソースタイプ: AWS::IAM::User

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iam-user-unused-credentials-check

AWS Identity and Access Management (IAM) ユーザーに、指定した日数内に使用されていないパスワードまたはアクティブなアクセスキーがあるかどうかを確認します。最近使用されていない非アクティブアカウントがある場合、ルールは NON_COMPLIANT です。

> **Note**
>
> 再評価タイムライン
> 最初の評価から 4 時間以内にこのルールを再評価しても結果には影響しません。
> マネージドルールとグローバル IAM リソースタイプ
> 2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および `AWS::IAM::User`) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョン

でのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降、 でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。
少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

識別子: IAM_USER_UNUSED_CREDENTIALS_CHECK

リソースタイプ: AWS::IAM::User

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

maxCredentialUsageAge, タイプ: int, デフォルト: 90

認証情報を使用できない最大日数。デフォルト値は 90 日です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

restricted-ssh

> **Important**
>
> このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。

セキュリティグループの受信 SSH トラフィックがアクセス可能かどうかを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。

識別子: INCOMING_SSH_DISABLED

リソースタイプ: AWS::EC2::SecurityGroup

トリガータイプ: 設定変更および定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

inspector-ec2-scan-enabled

EC2 インスタンスで潜在的な脆弱性とネットワーク到達可能性の問題を検出するために、Amazon Inspector V2 EC2 スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。EC2 スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: INSPECTOR_EC2_SCAN_ENABLED

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

inspector-ecr-scan-enabled

コンテナイメージの潜在的なソフトウェアの脆弱性を検出するために、Amazon Inspector V2 ECR スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。ECR スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: INSPECTOR_ECR_SCAN_ENABLED

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

inspector-lambda-code-scan-enabled

潜在的なコードの脆弱性を検出するために、Amazon Inspector V2 Lambda コードスキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。Lambda コードスキャンが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: INSPECTOR_LAMBDA_CODE_SCAN_ENABLED

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 欧州 (ストックホルム) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

inspector-lambda-standard-scan-enabled

ソフトウェアの潜在的な脆弱性を検出するために、Amazon Inspector V2 Lambda 標準スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。Lambda 標準スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: INSPECTOR_LAMBDA_STANDARD_SCAN_ENABLED

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ec2-instances-in-vpc

> **Important**
> このルールでは、ルール識別子 (IN_VPC) とルール名 (ec2-instances-in-vpc) が異なります。

EC2 インスタンスが Virtual Private Cloud (VPC) に属しているかどうかを確認します。オプションで、インスタンスに関連付ける VPC ID を指定できます。

識別子: INSTANCES_IN_VPC

リソースタイプ: AWS::EC2::Instance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

vpcId (オプション), 型: 文字列

これらの EC2 インスタンスが含まれている VPC ID。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

internet-gateway-authorized-vpc-only

インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされているかどうかを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

識別子: INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

リソースタイプ: AWS::EC2::InternetGateway

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS を除く、サポートされているすべての リージョン

パラメータ :

AuthorizedVpcIds (オプション), 型: 文字列

> 許可された VPC ID とアタッチされた IGW のカンマ区切りリスト。パラメータが指定されていない場合、アタッチされたすべての IGW は NON_COMPLIANT になります。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotevents-alarm-model-tagged

AWS IoT Events アラームモデルにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTEVENTS_ALARM_MODEL_TAGGED

リソースタイプ： AWS::IoTEvents::AlarmModel

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotevents-detector-model-tagged

AWS IoT Events ディテクターモデルにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTEVENTS_DETECTOR_MODEL_TAGGED

リソースタイプ： AWS::IoTEvents::DetectorModel

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotevents-input-tagged

AWS IoT Events 入力にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTEVENTS_INPUT_TAGGED

リソースタイプ： AWS::IoTEvents::Input

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotsitewise-asset-model-tagged

AWS IoT SiteWise アセットモデルにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTSITEWISE_ASSET_MODEL_TAGGED

リソースタイプ： AWS::IoTSiteWise::AssetModel

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotsitewise-dashboard-tagged

AWS IoT SiteWise ダッシュボードにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTSITEWISE_DASHBOARD_TAGGED

リソースタイプ： AWS::IoTSiteWise::Dashboard

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotsitewise-gateway-tagged

AWS IoT SiteWise ゲートウェイにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTSITEWISE_GATEWAY_TAGGED

リソースタイプ： AWS::IoTSiteWise::Gateway

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotsitewise-portal-tagged

AWS IoT SiteWise ポータルにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTSITEWISE_PORTAL_TAGGED

リソースタイプ： AWS::IoTSiteWise::Portal

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotsitewise-project-tagged

AWS IoT SiteWise プロジェクトにタグがあるかどうかを確認します。必要に応じて、ルールのタグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTSITEWISE_PROJECT_TAGGED

リソースタイプ： AWS::IoTSiteWise::Project

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iottwinmaker-component-type-tagged

AWS IoT TwinMaker コンポーネントタイプにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTTWINMAKER_COMPONENT_TYPE_TAGGED

リソースタイプ： AWS::IoTTwinMaker::ComponentType

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iottwinmaker-entity-tagged

AWS IoT TwinMaker エンティティにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTTWINMAKER_ENTITY_TAGGED

リソースタイプ： AWS::IoTTwinMaker::Entity

トリガータイプ: 設定変更

AWS リージョン： 欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iottwinmaker-scene-tagged

AWS IoT TwinMaker シーンにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTTWINMAKER_"_TAGGED

リソースタイプ： AWS::IoTTwinMaker::Scene

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iottwinmaker-sync-job-tagged

AWS IoT TwinMaker 同期ジョブにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTTWINMAKER_SYNC_JOB_TAGGED

リソースタイプ： AWS::IoTTwinMaker::SyncJob

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iottwinmaker-workspace-tagged

AWS IoT TwinMaker ワークスペースにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTTWINMAKER_WORKSPACE_TAGGED

リソースタイプ： AWS::IoTTwinMaker::Workspace

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotwireless-fuota-task-tagged

AWS IoT Wireless FUOTA タスクにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTWIRELESS_FUOTA_TASK_TAGGED

リソースタイプ： AWS::IoTWireless::FuotaTask

トリガータイプ: 設定変更

AWS リージョン： 欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotwireless-multicast-group-tagged

AWS IoT Wireless マルチキャストグループにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTWIRELESS_MULTICAST_GROUP_TAGGED

リソースタイプ： AWS::IoTWireless::MulticastGroup

トリガータイプ: 設定変更

AWS リージョン： 欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iotwireless-service-profile-tagged

AWS IoT Wireless サービスプロファイルにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IOTWIRELESS_SERVICE_PROFILE_TAGGED

リソースタイプ： AWS::IoTWireless::ServiceProfile

トリガータイプ: 設定変更

AWS リージョン： 欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シドニー) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

iot-authorizer-token-signing-enabled

AWS IoT Core オーソライザーが認可リクエストでトークン署名を検証するための署名要件を無効にしていないかどうかを確認します。オーソライザーに configuration.SigningDisabled が True に設定されている場合、ルールは NON_COMPLIANT です。

識別子： IOT_AUTHORIZER_TOKEN_SIGNING_ENABLED

リソースタイプ： AWS::IoT::Authorizer

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ivs-channel-playback-authorization-enabled

Amazon IVS チャネルで再生認可が有効になっているかどうかを確認します。configuration.Authorized が false の場合、ルールは NON_COMPLIANT です。

識別子： IVS_CHANNEL_PLAYBACK_AUTHORIZATION_ENABLED

リソースタイプ： AWS::IVS::Channel

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ivs-channel-tagged

Amazon IVS チャネルにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IVS_CHANNEL_TAGGED

リソースタイプ： AWS::IVS::Channel

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ivs-playback-key-pair-tagged

Amazon IVS 再生キーペアにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IVS_PLAYBACK_KEY_PAIR_TAGGED

リソースタイプ： AWS::IVS::PlaybackKeyPair

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ivs-recording-configuration-tagged

Amazon IVS 記録設定にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： IVS_RECORDING_CONFIGURATION_TAGGED

リソースタイプ： AWS::IVS::RecordingConfiguration

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック (東京) 、米国西部 (オレゴン) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

kinesis-firehose-delivery-stream-encrypted

Amazon Kinesis Data Firehose 配信ストリームがサーバー側の暗号化を使用して保存時に暗号化されているかどうかを確認します。Kinesis Data Firehose 配信ストリームがサーバー側の暗号化で保存時に暗号化されていない場合、ルールは NON_COMPLIANT です。

識別子: KINESIS_FIREHOSE_DELIVERY_STREAM_ENCRYPTED

リソースタイプ: AWS::KinesisFirehose::DeliveryStream

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

kmsKeyArns (オプション), タイプ: CSV

Kinesis Firehose の使用が承認されている KMS キー Arn のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

kinesis-stream-backup-retention-check

Amazon Kinesis Data Stream のデータレコード保持期間が特定の時間数に設定されているかどうかを確認します。プロパティ「RetentionPeriodHours」がパラメータで指定された値よりも短い場合、ルールは NON_COMPLIANT です。

識別子: KINESIS_STREAM_BACKUP_RETENTION_CHECK

リソースタイプ: AWS::Kinesis::Stream

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

minimumBackupRetentionPeriod (オプション), タイプ: 文字列

最小時間データレコードは保持する必要があります。有効な値は 24 ~ 8760、デフォルト値は 168 です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

kinesis-stream-encrypted

Amazon Kinesis Streams がサーバー側の暗号化を使用して保存時に暗号化されているかどうかを確認します。「StreamEncryption」が存在しない場合、ルールは Kinesis ストリームに対して NON_COMPLIANT になります。

コンテキスト: サーバー側の暗号化は、KMS キーを使用して保管前にデータを自動的に暗号化する Amazon Kinesis Data Streams AWS の機能です。データは、Kinesis ストリームストレージレイヤーに書き込まれる前に暗号化され、ストレージから取得された後で復号されます。その結果、Kinesis Data Streams サービス内で保管中のデータは暗号化されます。これは、規制要件を満たし、データのセキュリティを強化するために役立ちます。詳細については、「[Amazon Kinesis Data Streams のデータ保護](#)」を参照してください。

識別子: KINESIS_STREAM_ENCRYPTED

リソースタイプ: AWS::Kinesis::Stream

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

kms-cmk-not-scheduled-for-deletion

AWS Key Management Service (AWS KMS) キーが KMS AWS で削除されるようにスケジュールされていないかどうかを確認します。KMS キーを削除するようにスケジュールされている場合、ルールは NON_COMPLIANT です。

識別子: KMS_CMK_NOT_SCHEDULED_FOR_DELETION

リソースタイプ: AWS::KMS::Key

トリガータイプ: 定期的

AWS リージョン： 欧州 (ミラノ) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

kmsKeyIds (オプション), 型: 文字列

削除のスケジュールがされていない特定のカスタマーマネージド型キー ID のカンマ区切りリスト。キーを指定しない場合、ルールはすべてのキーを確認します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

kms-key-policy-no-public-access

KMS AWS キーポリシーでパブリックアクセスが許可されているかどうかを確認します。KMS キーポリシーが KMS キーへのパブリックアクセスを許可する場合、ルールは NON_COMPLIANT です。

> **Note**
>
> 非パブリックと見なされるには、KMS キーポリシーが固定値へのアクセスのみを許可する必要があります。つまり、ワイルドカードまたは次の IAM ポリシー要素を含まない値です: 変数。

識別子: KMS_KEY_POLICY_NO_PUBLIC_ACCESS

リソースタイプ: AWS::KMS::Key

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

lambda-concurrency-check

Lambda 関数に関数レベルの同時実行数制限が設定されているかどうかを確認します。Lambda 関数に関数レベルの同時実行数制限が設定されていない場合、ルールは NON_COMPLIANT です。

識別子: LAMBDA_CONCURRENCY_CHECK

リソースタイプ: AWS::Lambda::Function

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) 、中国 (寧夏) AWS を除くサポートされているすべての リージョン

パラメータ :

ConcurrencyLimitLow (オプション), 型: 文字列

同時実行数の下限

ConcurrencyLimitHigh (オプション), 型: 文字列

同時実行数の上限

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

lambda-dlq-check

Lambda 関数にデッドレターキューが設定されているかどうかを確認します。Lambda 関数にデッドレターキューが設定されていない場合、ルールは NON_COMPLIANT です。

識別子: LAMBDA_DLQ_CHECK

リソースタイプ: AWS::Lambda::Function

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) 、中国 (寧夏) AWS を除くサポートされているすべての リージョン

パラメータ :

dlqArns (オプション), 型: 文字列

Lambda 関数のデッドレターキューターゲットとして設定する必要がある Amazon SQS および Amazon SNS ARN のカンマ区切りリストです。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

lambda-function-public-access-prohibited

Lambda リソースにアタッチされた AWS Lambda 関数ポリシーがパブリックアクセスを禁止するかどうかを確認します。Lambda 関数ポリシーがパブリックアクセスを許可している場合、ルールは NON_COMPLIANT です。

コンテキスト: プリンシパル要素が空である、またはワイルドカードが含まれている場合、lambda 関数ポリシーはパブリックアクセスを許可すると見なされます。例えば、プリンシパル要素が `“”` または `{“AWS”: “”}` の場合です。セキュリティ上の理由から、パブリックアクセスの許可は推奨されていません。パブリックアクセスを制限すると、データが侵害されたり、不要なコストが発生する可能性がある Lambda 関数の不正な呼び出しを防ぐことができます。

Lambda 関数へのアクセスを制限するには、関数を呼び出すことができる IAM ユーザー、ロール、またはサービスの AWS アカウント IDs または Amazon リソースネーム (ARNs) を指定します。詳細については、「AWS Lambda デベロッパーガイド」の「関数へのアクセス権を他のアカウントに付与する」を参照してください。

このルールは`NON_COMPLIANT`、Lambda 関数が Amazon S3 から呼び出され、ポリシーに などのパブリックアクセスを制限する条件が含まれていない場合にも適用されます`AWS:SourceAccount`。より細かくアクセスするには、バケットポリシーで他の S3 条件を `AWS:SourceAccount` と併用することをおすすめします。

> **Note**
>
> 非公開と見なされるには、Lambda リソースベースのポリシーが固定値にのみアクセスを許可する必要があります。つまり、ワイルドカードまたは次の IAM ポリシー要素を含まない値です: 変数。

識別子: LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

リソースタイプ: AWS::Lambda::Function

トリガータイプ: 設定変更

AWS リージョン： 欧州 (スペイン) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

lambda-function-settings-check

ランタイム、ロール、タイムアウト、メモリサイズの AWS Lambda 関数設定が想定値と一致するかどうかを確認します。このルールは、「Image」パッケージタイプの関数と、「OS 専用ランタイム」に設定されたランタイムの関数を無視します。Lambda 関数の設定が期待値と一致しない場合、ルールは NON_COMPLIANT です。

識別子: LAMBDA_FUNCTION_SETTINGS_CHECK

リソースタイプ: AWS::Lambda::Function

トリガータイプ: 設定変更

AWS リージョン： 中国 (寧夏) AWS リージョンを除くサポートされているすべての リージョン

パラメータ :

ランタイム, タイプ: CSV

AWS Lambda ランタイム値のカンマ区切りリスト

ロール: (オプション), タイプ: 文字列

AWS Lambda 実行ロールの名前または ARN

タイムアウト (オプション), タイプ: int, デフォルト: 3

AWS Lambda 関数の秒単位のタイムアウト

memorySize (オプション), タイプ: int, デフォルト: 128

AWS メガバイト単位の Lambda 関数のサイズ

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

*これらの入力の有効な値の詳細については、 AWS CloudFormation 「 ユーザーガイド」のMemorySize、Role、Runtime、Timeout」を参照してください。

プロアクティブ評価の詳細については、「Evaluation Mode」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

lambda-function-xray-enabled

AWS Lambda 関数で AWS X-Ray が有効になっているかどうかを確認します。Lambda 関数で X-Ray トレースが無効になっている場合、ルールは NON_COMPLIANT です。

識別子： LAMBDA_FUNCTION_XRAY_ENABLED

リソースタイプ: AWS::Lambda::Function

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (ソウル) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

lambda-inside-vpc

Lambda 関数による仮想プライベートクラウド (VPC) へのアクセスが許可されているかどうかを確認します。Lambda 関数で VPC が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: LAMBDA_INSIDE_VPC

リソースタイプ: AWS::Lambda::Function

トリガータイプ: 設定変更

AWS リージョン： 中国 (寧夏) AWS リージョンを除くサポートされているすべての リージョン

パラメータ :

subnetIds (オプション), 型: 文字列

Lambda 関数に関連付けることができるサブネット ID のカンマ区切りリスト。

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、[AWS Config 「ルールを使用したリソースの評価](#)」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、[StartResourceEvaluation](#) API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
}
...
```

プロアクティブ評価の詳細については、「[評価モード](#)」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

lambda-vpc-multi-az-check

Lambda に複数のアベイラビリティーゾーンが関連付けられているかどうかを確認します。Lambda に 1 つのアベイラビリティーゾーンしか関連付けられていない場合、または関連付けられているアベイラビリティーゾーンの数がオプションのパラメータで指定されている数より少ない場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): LAMBDA_VPC_MULTI_AZ_CHECK

リソースタイプ: AWS::Lambda::Function

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

availabilityZones (オプション), タイプ: int

期待されるアベイラビリティーゾーンの数です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

lightsail-バケットタグ付き

Amazon Lightsail バケットにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： LIGHTSAIL_BUCKET_TAGGED

リソースタイプ： AWS::Lightsail::Bucket

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

lightsail-certificate-tagged

Amazon Lightsail 証明書にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： LIGHTSAIL_CERTIFICATE_TAGGED

リソースタイプ： AWS:Lightsail::Certificate

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴ

ン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

lightsail-disk-tagged

Amazon Lightsail ディスクにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： LIGHTSAIL_DISK_TAGGED

リソースタイプ： AWS:Lightsail::Disk

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

macie-auto-sensitive-data-discovery-check

Amazon Macie で機密データの自動検出が有効になっているかどうかを確認します。機密データの自動検出が無効になっている場合、ルールは NON_COMPLIANT です。このルールは管理者アカウントに適用され、メンバーアカウントには NOT_APPLICABLE です。

識別子: MACIE_AUTO_SENSITIVE_DATA_DISCOVERY_CHECK

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

macie-status-check

Amazon Macie がリージョンごとにアカウントで有効になっているかどうかを確認します。「status」属性が「ENABLED」に設定されていない場合、ルールは NON_COMPLIANT です。

[識別子:] MACIE_STATUS_CHECK

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mariadb-publish-logs-to-cloudwatch-logs

Amazon MariaDB データベースインスタンスが Amazon CloudWatch Logs にログを発行するように設定されているかどうかを確認します。データベースインスタンスが CloudWatch Logs にログを発行するように設定されていない場合、ルールは NON_COMPLIANT です。

識別子： MARIADB_PUBLISH_LOGS_TO_CLOUDWATCH_LOGS

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

logTypes (オプション), タイプ: 文字列

チェックするルールのログタイプのカンマ区切りリスト。指定しない場合、ルールはデフォルトのログタイプ「error」と「audit」をチェックします。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mfa-enabled-for-iam-console-access

コンソールパスワードを使用するすべての AWS Identity and Access Management (IAM) ユーザーに対して AWS 多要素認証 (MFA) が有効になっているかどうかを確認します。MFA が有効の場合、このルールは COMPLIANT です。

> **Note**
>
> 再評価タイムライン
> 最初の評価から 4 時間以内にこのルールを再評価しても結果には影響しません。
> マネージドルールとグローバル IAM リソースタイプ
> 2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および `AWS::IAM::User`) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降に でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、[AWS 「リソースの記録 | グローバルリソース](#)」を参照してください。
> 少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
> 不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、[「リージョンの可用性別の AWS Config マネージドルールのリスト](#)」を参照してください。

識別子: MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

リソースタイプ: AWS::IAM::User

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-active-broker-ldap-authentication

Amazon MQ ActiveMQ ブローカーが LDAP 認証戦略を使用してブローカーを保護するかどうかを確認します。configuration.AuthenticationStrategy が「ldap」でない場合、ルールは NON_COMPLIANT です。

識別子： MQ_ACTIVE_BROKER_LDAP_AUTHENTICATION

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-active-deployment-mode

Amazon MQ ActiveMQ ブローカーエンジンに設定されているデプロイモードを確認します。デフォルトの単一インスタンスブローカーモードが使用されている場合、ルールは NON_COMPLIANT です。

識別子: MQ_ACTIVE_DEPLOYMENT_MODE

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべてのリージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-active-single-instance-broker-storage-type-efs

mq.m5 インスタンスタイプファミリーを使用する Amazon MQ for ActiveMQ 単一インスタンスブローカーが、ブローカーストレージ用の Amazon Elastic File System (EFS) で設定されているかどう

かを確認します。configuration.StorageType が「efs」でない場合、ルールは NON_COMPLIANT です。

識別子： MQ_ACTIVE_SINGLE_INSTANCE_BROKER_STORAGE_TYPE_EFS

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-automatic-minor-version-upgrade-enabled

Amazon MQ ブローカーで自動マイナーバージョンアップグレードが有効かどうかを確認します。Amazon MQ ブローカーで「AutoMinorVersionUpgrade」フィールドが有効でない場合、ルールは NON_COMPLIANT です。

識別子: MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシ

フィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-auto-minor-version-upgrade-enabled

Amazon MQ ブローカーで自動マイナーバージョンアップグレードが有効かどうかを確認します。Amazon MQ ブローカーで「AutoMinorVersionUpgrade」フィールドが有効でない場合、ルールは NON_COMPLIANT です。

識別子: MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべてのリージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-broker-general-logging-enabled

Amazon MQ ブローカーで一般的なログ記録が有効になっているかどうかを確認します。configuration.Logs.General が false の場合、ルールは NON_COMPLIANT です。

識別子： MQ_BROKER_GENERAL_LOGGING_ENABLED

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-cloudwatch-audit-logging-enabled

Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっているかどうかを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

[識別子:] MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

[リソースタイプ:] AWS::AmazonMQ::Broker

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバー

ド) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-cloudwatch-audit-log-enabled

Amazon MQ ブローカーで CloudWatch 監査ログが有効になっているかどうかを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: MQ_CLOUDWATCH_AUDIT_LOG_ENABLED

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-no-public-access

Amazon MQ ブローカーがパブリックにアクセス可能ではないかどうかを確認します。Amazon MQ ブローカーで、「PubliclyAccessible」フィールドが true に設定されている場合、ルールは NON_COMPLIANT になります。

識別子: MQ_NO_PUBLIC_ACCESS

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アフリカ (ケープタウン) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

mq-rabbit-deployment-mode

Amazon MQ RabbitMQ ブローカーエンジンに設定されているデプロイモードを確認します。デフォルトの単一インスタンスブローカーモードが使用されている場合、ルールは NON_COMPLIANT です。

識別子: MQ_RABBIT_DEPLOYMENT_MODE

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

msk-cluster-public-access-disabled

Amazon MSK クラスターでパブリックアクセスが無効になっているかどうかを確認します。Amazon MSK クラスターのパブリックアクセスが無効になっていない場合、ルールは NON_COMPLIANT です。

識別子： MSK_CLUSTER_PUBLIC_ACCESS_DISABLED

リソースタイプ: AWS::MSK::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (ソウル) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべてのリージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

msk-connect-connector-logging-enabled

Amazon MSK Connector がログ送信先のいずれかに対してログ記録が有効になっているかどうかを確認します。Amazon MSK Connector でログ記録が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子： MSK_CONNECT_CONNECTOR_LOGGING_ENABLED

リソースタイプ： AWS::KafkaConnect::Connector

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

msk-enhanced-monitoring-enabled

拡張モニタリングが、PER_TOPIC_PER_BROKER または PER_TOPIC_PER_PARTITION に設定された Amazon MSK クラスターに対して有効になっているかどうかを確認します。拡張モニタリングが有効で、DEFAULT または PER_BROKER に設定されている場合、ルールは NON_COMPLIANT です。

識別子: MSK_ENHANCED_MONITORING_ENABLED

リソースタイプ: AWS::MSK::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

msk-in-cluster-node-require-tls

Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) を使用して転送中に暗号化を適用しているかどうかを確認します。プレーンテキスト通信がクラスター内ブローカーノード接続に対して有効になっている場合、ルールは NON_COMPLIANT です。

識別子: MSK_IN_CLUSTER_NODE_REQUIRE_TLS

リソースタイプ: AWS::MSK::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

msk-unrestricted-access-check

Amazon MSK クラスターで認証されていないアクセスが無効になっているかどうかを確認します。Amazon MSK クラスターで認証されていないアクセスが有効になっている場合、ルールは NON_COMPLIANT です。

識別子： MSK_UNRESTRICTED_ACCESS_CHECK

リソースタイプ: AWS::MSK::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (ソウル) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべてのリージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

multi-region-cloudtrail-enabled

> **Important**
>
> このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。

マルチリージョン AWS CloudTrail が少なくとも 1 つあるかどうかを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。`ExcludeManagementEventSources` フィールドが空でない場合、または AWS CloudTrail が AWS KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように設定されている場合、ルールは NON_COMPLIANT です。

識別子: MULTI_REGION_CLOUD_TRAIL_ENABLED

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

s3BucketNames (オプション), タイプ: 文字列

AWS CloudTrail がログファイルを配信する Amazon S3 バケットの名前。

snsTopicArn (オプション), タイプ: 文字列

通知に使用する AWS CloudTrail の Amazon SNS トピック ARN。

cloudWatchLogsLogGroupArn (オプション), タイプ: 文字列

CloudTrail がデータを送信する Amazon CloudWatch ロググループ ARN。 AWS CloudTrail

includeManagementEvents (オプション), タイプ：ブール値

AWS CloudTrail の管理イベントを含めるイベントセレクタ。

readWriteType (オプション), 型: 文字列

記録するイベントのタイプ。有効な値は、ReadOnly、WriteOnly、ALL です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

nacl-no-unrestricted-ssh-rdp

ネットワークアクセスコントロールリスト (NACL) の SSH/RDP 受信トラフィックに対するデフォルトポートが制限なしかどうかを確認します。NACL インバウンドエントリがポート 22 または 3389

についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): NACL_NO_UNRESTRICTED_SSH_RDP

リソースタイプ: AWS::EC2::NetworkAcl

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

neptune-cluster-backup-retention-check

Amazon Neptune DB クラスターの保持期間が特定の日数に設定されているかどうかを確認します。保持期間がパラメータで指定された値よりも短い場合、ルールは NON_COMPLIANT です。

識別子: NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

minimumBackupRetentionPeriod (オプション), タイプ: int

最低日数のバックアップを保存する必要があります。有効な値は 1 ~ 35 で、デフォルト値は 7 です。値が「backupRetentionPeriod」より大きい場合、ルールは NON_COMPLIANT です。値が「backupRetentionPeriod」以下の場合、ルールは COMPLIANT です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

neptune-cluster-cloudwatch-log-export-enabled

Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっているかどうかを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

neptune-cluster-copy-tags-to-snapshot-enabled

スナップショットの作成時に、すべてのタグをスナップショットにコピーするように Amazon Neptune クラスターが設定されているかどうかを確認します。「copyTagsToSnapshot」が false に設定されている場合、ルールは NON_COMPLIANT です。

識別子: NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

neptune-cluster-deletion-protection-enabled

Amazon Neptune DB クラスターの削除保護が有効になっているかどうかを確認します。Amazon Neptune クラスターの deletionProtection フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

識別子: NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシ

フィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

neptune-cluster-encrypted

Amazon Neptune DB クラスターでストレージ暗号化が有効になっているかどうかを確認します。ストレージの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: NEPTUNE_CLUSTER_ENCRYPTED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

KmsKeyArns (オプション), タイプ: CSV

暗号化されたクラスターの KmsKeyId と比較するための KMS キー ARN のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

neptune-cluster-iam-database-authentication

Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっているかどうかを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

neptune-cluster-multi-az-enabled

Amazon Neptune クラスターが Amazon RDS マルチ AZ レプリケーションを使用して設定されているかどうかを確認します。Multi-AZ のレプリケーションが有効でない場合、ルールは NON_COMPLIANT です。

識別子: NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

neptune-cluster-snapshot-encrypted

Amazon Neptune DB クラスターのスナップショットが暗号化されているかどうかを確認します。Neptune クラスターのスナップショットが暗号化されていない場合、ルールは NON_COMPLIANT です。

識別子: NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

リソースタイプ: AWS::RDS::DBClusterSnapshot

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

neptune-cluster-snapshot-public-prohibited

Amazon Neptune 手動 DB クラスタースナップショットがパブリックかどうかを確認します。既存および新規の Neptune スナップショットがパブリックの場合、ルールは NON_COMPLIANT です。

識別子: NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

リソースタイプ: AWS::RDS::DBClusterSnapshot

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

netfw-deletion-protection-enabled

AWS Network Firewall で削除保護が有効になっているかどうかを確認します。Network Firewall で削除保護が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: NETFW_DELETION_PROTECTION_ENABLED

リソースタイプ: AWS::NetworkFirewall::Firewall

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

netfw-logging-enabled

AWS Network Firewall ファイアウォールでログ記録が有効になっているかどうかを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

識別子: NETFW_LOGGING_ENABLED

リソースタイプ: AWS::NetworkFirewall::LoggingConfiguration

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

logType (オプション), タイプ: 文字列

> logType (オプション): ファイアウォールをチェックするルールのログタイプ: 「アラート」、「フロー」、または「両方」。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

netfw-multi-az-enabled

AWS Network Firewall ファイアウォールが複数のアベイラビリティーゾーンにデプロイされているかどうかを確認します。ファイアウォールが 1 つのアベイラビリティーゾーンにしかデプロイされていない場合、またはオプションのパラメータで指定されている数より少ないゾーンにデプロイされている場合、ルールは NON_COMPLIANT になります。

識別子: NETFW_MULTI_AZ_ENABLED

リソースタイプ: AWS::NetworkFirewall::Firewall

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

availabilityZones (オプション), タイプ: int

期待されるアベイラビリティーゾーンの数です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

netfw-policy-default-action-fragment-packets

AWS Network Firewall ポリシーが、フラグメント化されたパケットに対してユーザー定義のステートレスデフォルトアクションで設定されているかどうかを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

識別子: NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

リソースタイプ: AWS::NetworkFirewall::FirewallPolicy

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

statelessFragmentDefaultActions, タイプ: CSV

値のカンマ区切りリスト。最大 2 つを選択できます。有効な値には、「aws:pass」、「aws:drop」、「aws:forward_to_sfe」があります。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

netfw-policy-default-action-full-packets

AWS Network Firewall ポリシーが、フルパケットに対してユーザー定義のデフォルトのステートレスアクションで設定されているかどうかを確認します。完全なパケットのデフォルトステートレスアクションがユーザー定義のデフォルトステートレスアクションと一致しない場合、このルールは NON_COMPLIANT です。

識別子: NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

リソースタイプ: AWS::NetworkFirewall::FirewallPolicy

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

statelessDefaultActions, タイプ: CSV

値のカンマ区切りリスト。最大 2 つを選択できます。有効な値には、「aws:pass」、「aws:drop」、「aws:forward_to_sfe」があります。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

netfw-policy-rule-group-associated

AWS Network Firewall ポリシーがステートフルルールグループまたはステートレスルールグループに関連付けられていることを確認します。このルールは、ステートフルまたはステートレスルールグループが Network Firewall ポリシーに関連付けられていない場合、NON_COMPLIANT になります。いずれかのルールグループが存在する場合は COMPLIANT になります。

識別子: NETFW_POLICY_RULE_GROUP_ASSOCIATED

リソースタイプ: AWS::NetworkFirewall::FirewallPolicy

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

netfw-stateless-rule-group-not-empty

ステートレスネットワークファイアウォールのルールグループにルールが含まれているかどうかを確認します。ステートレスネットワークファイアウォールのルールグループにルールがない場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

リソースタイプ: AWS::NetworkFirewall::RuleGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

netfw-subnet-change-protection-enabled

AWS Network Firewall でサブネット変更保護が有効になっているかどうかを確認します。サブネット変更保護が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子： NETFW_SUBNET_CHANGE_PROTECTION_ENABLED

リソースタイプ: AWS::NetworkFirewall::Firewall

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

nlb-cross-zone-load-balancing-enabled

クロスゾーンロードバランシングが Network Load Balancer (NLB) に対して有効になっているかどうかを確認します。クロスゾーンロードバランシングが NLB に対して有効でない場合、このルールは NON_COMPLIANT になります。

識別子: NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

nlb-internal-scheme-check

Network Load Balancer スキームが内部的かどうかを確認します。configuration.scheme が内部に設定されていない場合、ルールは NON_COMPLIANT です。

識別子： NLB_INTERNAL_SCHEME_CHECK

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

nlb-listener-tagged

Network Load Balancer リスナーにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： NLB_LISTENER_TAGGED

リソースタイプ： AWS::ElasticLoadBalancingV2::Listener

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

nlb-logging-enabled

Network Load Balancer でアクセスログ記録が有効になっているかどうかを確認します。Network Load Balancer でアクセスログ記録が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子： NLB_LOGGING_ENABLED

リソースタイプ: AWS::ElasticLoadBalancingV2::LoadBalancer

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

no-unrestricted-route-to-igw

ルートテーブルにインターネットゲートウェイ (IGW) へのパブリックルートがあるかどうかを確認します。IGW へのルートに「0.0.0.0/0」または「:: /0」などの送信先 CIDR ブロックがある場合、ま

たは送信先 CIDR ブロックがルールパラメータと一致しない場合、ルールは NON_COMPLIANT です。

識別子: NO_UNRESTRICTED_ROUTE_TO_IGW

リソースタイプ: AWS::EC2::RouteTable

トリガータイプ: 設定変更および定期的

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

routeTableIds (オプション), タイプ: CSV

「0.0.0.0/0」または「:: /0」などの送信先 CIDR ブロックがあるインターネットゲートウェイへのルートを持つことができるルートテーブル ID のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-access-control-enabled

きめ細かなアクセスコントロールが Amazon OpenSearch Service ドメインに設定されているかどうかをチェックします。AdvancedSecurityOptions が OpenSearch Service ドメインに対して有効になっていない場合、ルールは NON_COMPLIANT です。

[Identifier:] (識別子:) OPENSEARCH_ACCESS_CONTROL_ENABLED

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中

国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-audit-logging-enabled

Amazon OpenSearch Service ドメインで監査ログが有効になっているかどうかを確認します。OpenSearch Service ドメインで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: OPENSEARCH_AUDIT_LOGGING_ENABLED

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

cloudWatchLogsLogGroupArnList (オプション), タイプ: CSV

Amazon CloudWatch Logs ロググループの Amazon リソースネーム (ARN) のカンマ区切りリストです。このルールは、指定されたロググループが監査ログに設定されているかどうかを確認します。

有効な値には、`arn:aws:logs:region:account-id:log-group:log_group_name:*` や `arn:aws:logs:region:account-id:log-group:log_group_name` などがあります。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-data-node-fault-tolerance

Amazon OpenSearch Serviceのドメインが少なくとも 3 つのデータノードで構成され、zoneAwarenessEnabled が true であるかどうかをチェックします。'instanceCount' が 3 より小さい場合、または 'zoneAwarenessEnabled' が 'false' に設定されている場合、OpenSearch ドメインのルールは NON_COMPLIANT です。

[Identifier:] (識別子:) OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-encrypted-at-rest

Amazon OpenSearch Service ドメインで保管時の暗号化設定が有効になっているかどうかを確認します。`EncryptionAtRestOptions` フィールドが有効でない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> このルールは Elasticsearch ドメインを評価しません。

[Identifier:] (識別子:) OPENSEARCH_ENCRYPTED_AT_REST

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-https-required

OpenSearch ドメインへの接続が HTTPS を使用しているかどうかをチェックします。Amazon OpenSearch ドメイン 'EnforceHTTPS' が 'true' でない場合、または 'true' であって 'TLSSecurityPolicy' が '`tlsPolicies`' でない場合、ルールは NON_COMPLIANT です。

[Identifier:] (識別子:) OPENSEARCH_HTTPS_REQUIRED

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボ

ルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

tlsPolicies (オプション), タイプ: CSV

Amazon OpenSearch ドメインに対してチェックする TLS セキュリティポリシーのカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-in-vpc-only

Amazon OpenSearch Service ドメインが Amazon Virtual Private Cloud (Amazon VPC) 内にあるかどうかを確認します。OpenSearch Service ドメインのエンドポイントがパブリックである場合、ルールは NON_COMPLIANT になります。

> **Note**
>
> このルールは Elasticsearch ドメインを評価しません。

[Identifier] (識別子): OPENSEARCH_IN_VPC_ONLY

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン : 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-logs-to-cloudwatch

Amazon OpenSearch Service ドメインが、Amazon CloudWatch Logs にログを送信するように設定されているかどうかを確認します。ログ記録が設定されていない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> このルールは Elasticsearch ドメインを評価しません。

[Identifier:] (識別子:) OPENSEARCH_LOGS_TO_CLOUDWATCH

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

logTypes (オプション), タイプ: CSV

有効になっているログのカンマ区切りリスト。有効な値は 「search」、「index」、「error」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-node-to-node-encryption-check

Amazon OpenSearch Service ノードがエンドツーエンドで暗号化されているかどうかを確認します。ノード間の暗号化がドメイン上で有効になっていない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> このルールは Elasticsearch ドメインを評価しません。

[Identifier:] (識別子:) OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-primary-node-fault-tolerance

Amazon OpenSearch Service ドメインが少なくとも 3 つの専用プライマリノードで構成されているかどうかを確認します。「DedicatedMasterEnabled」が「false」に設定されている場合、または「DedicatedMasterCount」が 3 未満である場合、OpenSearch Service ドメインのルールは NON_COMPLIANT です。

識別子: OPENSEARCH_PRIMARY_NODE_FAULT_TOLERANCE

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

opensearch-update-check

Amazon OpenSearch Service バージョンのアップデートが利用可能であるものの、インストールされていないことを確認します。最新のソフトウェアの更新がインストールされていない場合、OpenSearch ドメインのルールは NON_COMPLIANT です。

識別子: OPENSEARCH_UPDATE_CHECK

リソースタイプ: AWS::OpenSearch::Domain

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rabbit-mq-supported-version

Amazon MQ RabbitMQ ブローカーが、指定された最小サポートエンジンバージョンで実行されているかどうかを確認します。RabbitMQ ブローカーが、指定した最小サポートエンジンバージョンで実行されていない場合、ルールは NON_COMPLIANT です。

識別子: RABBIT_MQ_SUPPORTED_VERSION

リソースタイプ: AWS::AmazonMQ::Broker

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

supportedEngineVersion, タイプ: 文字列

RabbitMQ ブローカーでサポートされている最小エンジンバージョンをチェックするルールの文字列値。RabbitMQ ブローカーはセマンティックバージョニング仕様を使用します。X、Y、Z、X はメジャーバージョン、Y はマイナーバージョン、Z はパッチバージョンを表します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-aurora-mysql-audit-logging-enabled

Amazon Aurora MySQL 互換エディションのクラスターが監査ログを Amazon CloudWatch Logs に発行するように設定されているかどうかを確認します。Aurora MySQL 互換エディションのクラスターで、監査ログの公開が有効でない場合、ルールは NON_COMPLIANT です。

識別子: RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-aurora-postgresql-logs-to-cloudwatch

Amazon Aurora PostgreSQL DB クラスターがPostgreSQL ログを Amazon CloudWatch Logs に発行するように設定されているかどうかを確認します。DB クラスターが PostgreSQL ログを Amazon CloudWatch Logs に発行するように設定されていない場合、このルールは NON_COMPLIANT です。

識別子: RDS_AURORA_POSTGRESQL_LOGS_TO_CLOUDWATCH

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-automatic-minor-version-upgrade-enabled

Amazon Relational Database Service (Amazon RDS) データベースインスタンスが、自動マイナーバージョンアップグレードに設定されているかどうかを確認します。「autoMinorVersionUpgrade」の値が false の場合、ルールは NON_COMPLIANT です。

識別子: RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

なし

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、[AWS Config 「ルールを使用したリソースの評価](#)」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すに

は、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

*これらの入力の有効な値の詳細については、「 AWS CloudFormation ユーザーガイド」のAutoMinorVersionUpgrade」と「 エンジン」を参照してください。

プロアクティブ評価の詳細については、「Evaluation Mode」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

rds-cluster-auto-minor-version-upgrade-enable

Amazon RDS マルチ AZ クラスターデプロイで自動マイナーバージョンアップグレードが有効になっているかどうかを確認します。autoMinorVersionUpgrade の値が false の場合、ルールは NON_COMPLIANT です。

識別子: RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、米国西部 (北カリフォルニア) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-cluster-default-admin-check

Amazon Relational Database Service (Amazon RDS) データベースクラスターが管理者ユーザーネームをそのデフォルト値から変更したかどうかを確認します。管理者ユーザーネームがデフォルト値に設定されている場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): RDS_CLUSTER_DEFAULT_ADMIN_CHECK

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

validAdminUserNames (オプション), タイプ: CSV

> Amazon RDS クラスターが使用できる管理者ユーザーネームのコンマ区切りのリストです。「postgres」と「admin」はデフォルト値であるため、有効なユーザーネームとしてこれらのいずれかを含めることはできません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-cluster-deletion-protection-enabled

Amazon Relational Database Service (Amazon RDS) クラスターで削除保護が有効になっているかどうかを確認します。Amazon RDS クラスターで削除保護が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: RDS_CLUSTER_DELETION_PROTECTION_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-cluster-encrypted-at-rest

Amazon Relational Database Service (Amazon RDS) クラスターが保管時に暗号化されているかどうかを確認します。Amazon RDS クラスターが保管時に暗号化されていない場合、ルールは NON_COMPLIANT です。

Identifier: RDS_CLUSTER_ENCRYPTED_AT_REST

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-cluster-iam-authentication-enabled

Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっているかどうかを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-cluster-multi-az-enabled

Amazon Relational Database Service (Amazon RDS) によって管理される Amazon Aurora およびマルチ AZ DB クラスターでマルチアベイラビリティーゾーン (マルチ AZ) レプリケーションが有効になっているかどうかを確認します。Amazon RDS インスタンスがマルチ AZ を使用して設定されていない場合、ルールは NON_COMPLIANT です。

識別子: RDS_CLUSTER_MULTI_AZ_ENABLED

リソースタイプ: AWS::RDS::DBCluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (メルボルン) AWS を除くサポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-db-security-group-not-allowed

デフォルトの DB セキュリティグループではない Amazon Relational Database Service (Amazon RDS) DB セキュリティグループが存在するかどうかを確認します。デフォルトの DB セキュリティグループではない DB セキュリティグループが存在する場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): RDS_DB_SECURITY_GROUP_NOT_ALLOWED

リソースタイプ: AWS::RDS::DBSecurityGroup

トリガータイプ: 設定変更

AWS リージョン: 欧州 (アイルランド)、南米 (サンパウロ)、米国東部 (バージニア北部)、アジアパシフィック (東京)、米国西部 (オレゴン)、米国西部 (北カリフォルニア)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー) リージョンのみで利用可能です。

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-enhanced-monitoring-enabled

Amazon RDS インスタンスに対して拡張モニタリングが有効になっているかどうかをチェックします。RDS インスタンスの設定項目で「`monitoringInterval`」が「`0`」の場合、または「`monitoringInterval`」がルールパラメータ値と一致しない場合、このルールは NON_COMPLIANT です。

識別子: RDS_ENHANCED_MONITORING_ENABLED

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

monitoringInterval (オプション), タイプ: int

> データベースインスタンスに対して拡張モニタリングメトリクスが収集される場合のポイント間の整数値 (秒)。有効な値は、1、5、10、15、30、および 60 です。

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

*これらの入力の有効な値の詳細については、「 AWS CloudFormation ユーザーガイド」のMonitoringInterval and Engine」を参照してください。

プロアクティブ評価の詳細については、「Evaluation Mode」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-instance-default-admin-check

Amazon Relational Database Service (Amazon RDS) データベースが管理者ユーザーネームをそのデフォルト値から変更したかどうかを確認します。このルールが実行されるのは RDS データベースインスタンスのみです。管理者ユーザーネームがデフォルト値に設定されている場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): RDS_INSTANCE_DEFAULT_ADMIN_CHECK

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

validAdminUserNames (オプション), タイプ: CSV

> Amazon RDS インスタンスが使用できる管理者ユーザーネームのカンマ区切りのリストです。(「postgres」と「admin」はデフォルト値であるため、有効なユーザーネームとしてこれらのいずれかを含めることはできません。)

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-instance-deletion-protection-enabled

Amazon Relational Database Service (Amazon RDS) インスタンスで削除保護が有効になっているかどうかを確認します。Amazon RDS インスタンスで削除保護が有効になっていない場合、つまり deletionProtection が false に設定されている場合、ルールは NON_COMPLIANT です。

> **Warning**
> クラスター内の一部の RDS DB インスタンス (Aurora/DocumentDB) は、非準拠として表示されます。

識別子: RDS_INSTANCE_DELETION_PROTECTION_ENABLED

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

databaseEngines (オプション), タイプ: CSV

ルールの評価に含める RDS データベースエンジンのカンマ区切りリスト。例:「mysql, postgres, mariadb」

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-instance-iam-authentication-enabled

Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっているかどうかを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

> **Note**
> DB エンジンは「mysql」、「postgres」、「aurora」、「aurora-mysql」、「aurora-postgresql」のいずれかである必要があります。DB インスタンスのステータスは、「available」(使用可能)、「backing-up」(バックアップ中)、「storage-optimization」(ストレージ最適化)、「storage-full」(ストレージ不足) のいずれかである必要があります。

識別子: RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-instance-public-access-check

Amazon Relational Database Service (Amazon RDS) インスタンスがパブリックアクセス可能になっていないかどうかを確認します。インスタンスの設定項目で publiclyAccessible フィールドが true の場合、ルールは NON_COMPLIANT です。

識別子: RDS_INSTANCE_PUBLIC_ACCESS_CHECK

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、[AWS Config 「ルールを使用したリソースの評価](#)」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、[StartResourceEvaluation](#) API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

rds-instance-subnet-igw-check

RDS DB インスタンスがインターネットゲートウェイへのルートを持つパブリックサブネットにデプロイされているかどうかを確認します。RDS DB インスタンスがパブリックサブネットにデプロイされている場合、ルールは NON_COMPLIANT です

識別子： RDS_INSTANCE_SUBNET_IGW_CHECK

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： AWS 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

rds-in-backup-plan

Amazon Relational Database Service (Amazon RDS) データベースが AWS Backup プランに存在するかどうかを確認します。Amazon RDS データベースが AWS Backup プランに含まれていない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> ルールは Amazon Aurora DB インスタンスにのみ適用されます。DB クラスターはサポートされません。

識別子: RDS_IN_BACKUP_PLAN

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-last-backup-recovery-point-created

Amazon Relational Database Service (Amazon RDS) のリカバリポイントが作成されたかどうかを確認します。Amazon RDS インスタンスに対応するリカバリポイントが指定した期間内に作成されていない場合、ルールは NON_COMPLIANT です。

識別子: RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon RDS インスタンスのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon RDS インスタンスの ID

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-logging-enabled

Amazon Relational Database Service (Amazon RDS) の各ログが有効になっているかどうかを確認します。どのログタイプも有効でない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> 「使用可能」、「バックアップ中」、「ストレージ最適化」、または「ストレージ不足」の状態でない DB インスタンスは、`NOT_APPLICABLE` と評価されます。

識別子: RDS_LOGGING_ENABLED

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

additionalLogs (オプション), 型: StringMap

エンジン名とログタイプ名のカンマ区切りリスト。例: "additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-mariadb-instance-encrypted-in-transit

エンジンバージョン 10.5 以上の Amazon RDS for MariaDB DB インスタンスへの接続が転送中の暗号化を使用しているかどうかを確認します。DB パラメータグループが同期していない場合、または require_secure_transport が ON に設定されていない場合、ルールは NON_COMPLIANT です。

識別子： RDS_MARIADB_INSTANCE_ENCRYPTED_IN_TRANSIT

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-meets-restore-time-target

Amazon Relational Database Service (Amazon RDS) インスタンスの復元時間が、指定された期間と一致しているかどうかを確認します。Amazon RDS インスタンスの LatestRestoreExecutionTimeMinutes が maxRestoreTime の値より大きい場合、ルールは NON_COMPLIANT です。

識別子: RDS_MEETS_RESTORE_TIME_TARGET

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

maxRestoreTime, タイプ: int

最大許容復元ランタイムの数値。

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon RDS インスタンスのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon RDS インスタンスの ID

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-multi-az-support

RDS DB インスタンスの高可用性が有効になっているかどうかを確認します。

Amazon RDS のマルチ AZ 配置では、異なるアベイラビリティーゾーンに同期スタンバイレプリカが自動的にプロビジョニングされて維持されます。詳細については、Amazon RDS ユーザーガイドの高可用性 (マルチ AZ) を参照してください。

> **Note**
>
> このルールは、Amazon Aurora DB インスタンス、Amazon DocumentDB インスタンス、および Amazon Neptune DB インスタンスを評価しません。

識別子: RDS_MULTI_AZ_SUPPORT

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

*これらの入力の有効な値の詳細については、 AWS CloudFormation 「 ユーザーガイド」のMultiAZ and Engine」を参照してください。

プロアクティブ評価の詳細については、「Evaluation Mode」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

rds-mysql-instance-encrypted-in-transit

Amazon RDS for MySQL データベースインスタンスへの接続が、転送中の暗号化を使用するように設定されているかどうかを確認します。関連付けられたデータベースパラメータグループが同期していない場合、または require_secure_transport パラメータが 1 に設定されていない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> Amazon RDS インスタンスが RDS クラスターの一部`NOT_APPLICABLE`である場合、ルールは を返します。

識別子: RDS_MYSQL_INSTANCE_ENCRYPTED_IN_TRANSIT

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

rds-postgresql-logs-to-cloudwatch

Amazon PostgreSQL DB インスタンスが Amazon CloudWatch Logs にログを発行するように設定されているかどうかを確認します。DB インスタンスが Amazon CloudWatch Logs にログを発行するように設定されていない場合、ルールは NON_COMPLIANT です。

識別子: RDS_POSTGRESQL_LOGS_TO_CLOUDWATCH

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

logTypes (オプション), タイプ: CSV

CloudWatch Logs に発行するログタイプのカンマ区切りリスト。有効な値は、「postgresql」、「upgrade」です。デフォルト値は「postgresql」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-postgres-instance-encrypted-in-transit

Amazon RDS PostgreSQL データベースインスタンスへの接続が、転送中の暗号化を使用するように設定されているかどうかを確認します。関連付けられたデータベースパラメータグループが同期していない場合、または rds.force_ssl パラメータが 1 に設定されていない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> Amazon RDS インスタンスが RDS クラスターの一部`NOT_APPLICABLE`である場合、ルールは を返します。

識別子: RDS_POSTGRES_INSTANCE_ENCRYPTED_IN_TRANSIT

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-proxy-tls-encryption

Amazon RDS プロキシがすべての接続に TLS を適用するかどうかを確認します。Amazon RDS プロキシにすべての接続に TLS が適用されていない場合、ルールは NON_COMPLIANT です。

識別子： RDS_PROXY_TLS_ENCRYPTION

リソースタイプ： AWS::RDS::DBProxy

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-resources-protected-by-backup-plan

Amazon Relational Database Service (Amazon RDS) インスタンスがバックアップ計画で保護されているかどうかを確認します。Amazon RDS データベースインスタンスがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

識別子:RDS_RESOURCES_PROTECTED_BACKUP_PLAN

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon RDS インスタンスのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)

resourceId (オプション), 型: 文字列

チェックするルールの Amazon RDS インスタンスの ID

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-snapshots-public-prohibited

Amazon Relational Database Service (Amazon RDS) スナップショットがパブリックかどうかを確認します。既存および新規の Amazon RDS スナップショットがパブリックである場合、ルールは NON_COMPLIANT です。

> **Note**
> コンプライアンス結果の取得には、最大 12 時間かかることがあります。

識別子: RDS_SNAPSHOTS_PUBLIC_PROHIBITED

リソースタイプ: AWS::RDS::DBSnapshot、AWS::RDS::DBClusterSnapshot

トリガータイプ: 設定変更

AWS リージョン： AWS アフリカ (ケープタウン) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) 、イスラエル (テルアビブ) 、欧州 (スペイン) 、欧州 (チューリッヒ) を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-snapshot-encrypted

Amazon Relational Database Service (Amazon RDS) DB スナップショットが暗号化されているかどうかを確認します。Amazon RDS DB スナップショットが暗号化されていない場合、ルールは NON_COMPLIANT です。

識別子: RDS_SNAPSHOT_ENCRYPTED

リソースタイプ: AWS::RDS::DBSnapshot、AWS::RDS::DBClusterSnapshot

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-sqlserver-encrypted-in-transit

Amazon RDS SQL Server データベースインスタンスへの接続が、転送中の暗号化を使用するように設定されているかどうかを確認します。パラメータグループの DB パラメータ force_ssl が 1 に設定されていない場合、または ApplyStatus パラメータが「in-sync」でない場合、ルールは NON_COMPLIANT です。

識別子： RDS_SQLSERVER_ENCRYPTED_IN_TRANSIT

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 定期的

AWS リージョン： AWS 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

rds-sql-server-logs-to-cloudwatch

Amazon SQL Server DB インスタンスが Amazon CloudWatch Logs にログを発行するように設定されているかどうかを確認します。DB インスタンスが Amazon CloudWatch Logs にログを発行するように設定されていない場合、このルールは NON_COMPLIANT です。

識別子: RDS_SQL_SERVER_LOGS_TO_CLOUDWATCH

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

logTypes (オプション), タイプ: CSV

> logTypes - (オプション): CloudWatch Logs に発行するログタイプのカンマ区切りリスト。有効な値は「error」、「agent」です。デフォルト値は「error」、「agent」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

rds-storage-encrypted

Amazon Relational Database Service (Amazon RDS) DB インスタンスでストレージの暗号化が有効になっているかどうかを確認します。ストレージの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: RDS_STORAGE_ENCRYPTED

リソースタイプ: AWS::RDS::DBInstance

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

kmsKeyId (オプション), タイプ: 文字列

ストレージの暗号化に使用する KMS キー ID または Amazon リソースネーム (ARN)。

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-audit-logging-enabled

Amazon Redshift クラスターが特定のバケットに対する監査を記録しているかどうかを確認します。Redshift クラスターに対して監査ログが有効化されていない場合、または「`bucketNames`」パラメータが指定されているが、監査ログの送信先が一致しない場合、ルールは NON_COMPLIANT になります。

識別子: REDSHIFT_AUDIT_LOGGING_ENABLED

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

bucketNames (オプション), タイプ: CSV

監査ログを保存するための Amazon S3 バケット名のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-backup-enabled

Amazon Redshift 自動スナップショットがクラスターに対して有効になっていることを確認します。`automatedSnapshotRetentionPeriod` の値が `MaxRetentionPeriod` より大きいか

`MinRetentionPeriod` より小さい場合、または値が 0 の場合、ルールは NON_COMPLIANT です。

識別子: REDSHIFT_BACKUP_ENABLED

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

MinRetentionPeriod (オプション), タイプ: int

保持期間の最小値。最小値は 1 です。

MaxRetentionPeriod (オプション), タイプ: int

保持期間の最大値。最大値は 35 です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-cluster-configuration-check

Amazon Redshift クラスターに指定された設定があるかどうか確認します。Amazon Redshift クラスターが暗号化されていない、または別のキーで暗号化されている場合、または監査ログ作成が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: REDSHIFT_CLUSTER_CONFIGURATION_CHECK

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック

(台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

clusterDbEncrypted, 型: ブール値, デフォルト: true

データベースの暗号化は有効になっています。

loggingEnabled, 型: ブール値, デフォルト: true

監査ログ記録は有効になっています。

nodeTypes (オプション), タイプ: CSV, デフォルト: dc1.large

ノードの種類を指定します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-cluster-kms-enabled

Amazon Redshift クラスターが暗号化に指定された AWS Key Management Service （ AWS KMS) キーを使用しているかどうかを確認します。暗号化が有効になっていて、クラスターが `kmsKeyArn` パラメータで指定されたキーで暗号化されている場合、ルールは COMPLIANT です。クラスターが暗号化されていない場合、または別のキーで暗号化されている場合、ルールは NON_COMPLIANT です。

識別子: REDSHIFT_CLUSTER_KMS_ENABLED

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

kmsKeyArns (オプション), タイプ: CSV

暗号化のために Amazon Redshift クラスターで使用される AWS KMS キー Amazon リソースネーム (ARNs) のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

redshift-cluster-maintenancesettings-check

Amazon Redshift クラスターに、指定されたメンテナンス設定があるかどうか確認します。メジャーバージョンへの自動アップグレードが無効になっている場合、ルールは NON_COMPLIANT です。

識別子: REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

allowVersionUpgrade, 型: ブール値, デフォルト: true

バージョンアップグレードの許可が有効になっています。

preferredMaintenanceWindow (オプション), 型: 文字列

クラスターのスケジュールされたメンテナンスウィンドウ (例: Mon:09:30-Mon:10:00)。

automatedSnapshotRetentionPeriod (オプション), タイプ: int, デフォルト: 1

自動スナップショットを保持する日数。

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すに

は、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

*これらの入力の有効な値の詳細については、 AWS CloudFormation ユーザーガイドのAutomatedSnapshotRetentionPeriod」、PreferredMaintenanceWindow」、およびAllowVersionUpgrade」を参照してください。

プロアクティブ評価の詳細については、「Evaluation Mode」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

redshift-cluster-multi-az-enabled

Amazon Redshift クラスターで複数のアベイラビリティーゾーンのデプロイが有効になっているかどうかを確認します。Amazon Redshift クラスターで複数のアベイラビリティーゾーンデプロイが有効になっていない場合、このルールは NON_COMPLIANT です。

識別子： REDSHIFT_CLUSTER_MULTI_AZ_ENABLED

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (ソウル) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、米国西部 (北カリフォルニア) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-cluster-parameter-group-tagged

Amazon Redshift クラスターパラメータグループにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： REDSHIFT_CLUSTER_PARAMETER_GROUP_TAGGED

リソースタイプ： AWS::Redshift::ClusterParameterGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-cluster-public-access-check

Amazon Redshift クラスターがパブリックアクセス可能になっていないかどうかを確認します。クラスターの設定項目で publiclyAccessible フィールドが True の場合、ルールは NON_COMPLIANT です。

Identifier: REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

redshift-cluster-subnet-group-multi-az

Amazon Redshift サブネットグループに複数のアベイラビリティーゾーンからのサブネットが含まれているかどうかを確認します。Amazon Redshift サブネットグループに少なくとも 2 つの異なるアベイラビリティーゾーンからのサブネットが含まれていない場合、ルールは NON_COMPLIANT です。

識別子: REDSHIFT_CLUSTER_SUBNET_GROUP_MULTI_AZ

リソースタイプ: AWS::Redshift::ClusterSubnetGroup

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-default-admin-check

Amazon Redshift クラスターが管理者ユーザーネームをそのデフォルト値から変更したかどうかを確認します。Redshift クラスターの管理ユーザーネームが「awsuser」に設定されている、またはユーザーネームがパラメータにリストされているものと一致しない場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): REDSHIFT_DEFAULT_ADMIN_CHECK

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

validAdminUserNames (オプション), タイプ: CSV

Redshift クラスターが使用する管理者ユーザーネームのコンマ区切りのリストです。注意: 「awsuser」はデフォルト値で、受け入れられません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-default-db-name-check

Redshift クラスターがデータベース名をそのデフォルト値から変更したかどうかを確認します。Redshift クラスターのデータベース名が「dev」に設定されている場合、またはオプションのパラメータが指定されているのにデータベース名が一致しない場合、ルールは NON_COMPLIANT です。

識別子: REDSHIFT_DEFAULT_DB_NAME_CHECK

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

validDatabaseNames (オプション), タイプ: CSV

Redshift クラスターのデータベース名のカンマ区切りのリストです。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-enhanced-vpc-routing-enabled

Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっているかどうかを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。

識別子: REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-require-tls-ssl

Amazon Redshift クラスターで SQL クライアントに接続するための TLS/SSL 暗号化が必要かどうかを確認します。Amazon Redshift クラスターでパラメータの require_SSL が true に設定されていない場合、ルールは NON_COMPLIANT です。

識別子: REDSHIFT_REQUIRE_TLS_SSL

リソースタイプ: AWS::Redshift::Cluster、AWS::Redshift::ClusterParameterGroup

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-serverless-default-admin-check

Amazon Redshift Serverless 名前空間が管理者ユーザー名をデフォルト値から変更したかどうかを確認します。Redshift Serverless 名前空間の管理者ユーザー名が「admin」に設定されている場合、ルールは NON_COMPLIANT です。

識別子： REDSHIFT_SERVERLESS_DEFAULT_ADMIN_CHECK

リソースタイプ： AWS::RedshiftServerless::Namespace

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アフリカ (ケープタウン) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-serverless-default-db-name-check

Amazon Redshift Serverless 名前空間がデータベース名をデフォルト値から変更したかどうかを確認します。Amazon Redshift Serverless 名前空間のデータベース名が「dev」に設定されている場合、ルールは NON_COMPLIANT です。

識別子： REDSHIFT_SERVERLESS_DEFAULT_DB_NAME_CHECK

リソースタイプ： AWS::RedshiftServerless::Namespace

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アフリカ (ケープタウン) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべてのリージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-serverless-namespace-cmk-encryption

Amazon Redshift Serverless 名前空間がカスタマーマネージド KMS AWS キーによって暗号化されているかどうかを確認します。名前空間がカスタマーマネージドキーによって暗号化されていない場合、ルールは NON_COMPLIANT です。必要に応じて、チェックするルールの KMS キーのリストを指定できます。

識別子： REDSHIFT_SERVERLESS_NAMESPACE_CMK_ENCRYPTION

リソースタイプ： AWS::RedshiftServerless::Namespace

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アフリカ (ケープタウン) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべてのリージョン

パラメータ：

kmsKeyArns (オプション), タイプ: CSV

チェックするルールのカスタマーマネージドキーの Amazon リソースネーム (ARNs) のカンマ区切りリスト。指定した場合、Amazon Redshift Serverless 名前空間がこれらの KMS キーのいずれかで暗号化されていない場合、ルールは NON_COMPLIANT です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-serverless-publish-logs-to-cloudwatch

Amazon Redshift Serverless Namespace が Amazon CloudWatch Logs に次のログを発行するように設定されているかどうかを確認します。名前空間が Amazon CloudWatch Logs に次のログを発行するように設定されていない場合、このルールは NON_COMPLIANT です。

識別子： REDSHIFT_SERVERLESS_PUBLISH_LOGS_TO_CLOUDWATCH

リソースタイプ： AWS::RedshiftServerless::Namespace

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アフリカ (ケープタウン) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

logType (オプション), タイプ: CSV

CloudWatch Logs に発行するログタイプのカンマ区切りリスト。有効な値は「connectionlog」、「userlog」です。デフォルト値は「connectionlog」、「userlog」です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-serverless-workgroup-encrypted-in-transit

AWS Redshift Serverless ワークグループの require_ssl 設定パラメータが true に設定されているかどうかを確認します。require_ssl が false に設定されている場合、ルールは NON_COMPLIANT です。

識別子： REDSHIFT_SERVERLESS_WORKGROUP_ENCRYPTED_IN_TRANSIT

リソースタイプ： AWS::RedshiftServerless::Workgroup

トリガータイプ: 定期的

AWS リージョン： 欧州 (ストックホルム) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) 、欧州 (スペイン) 、欧州 (チューリッヒ) リージョンでのみ利用可能

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-serverless-workgroup-no-public-access

Amazon Redshift Serverless ワークグループがパブリックアクセスを許可していないかどうかを確認します。ワークグループで「パブリックアクセス可能をオンにする」が有効になっている場合、ルールは NON_COMPLIANT です。

識別子： REDSHIFT_SERVERLESS_WORKGROUP_NO_PUBLIC_ACCESS

リソースタイプ： AWS::RedshiftServerless::Workgroup

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (タイ) 、アフリカ (ケープタウン) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、欧州 (ミラノ) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-serverless-workgroup-routes-within-vpc

Amazon Redshift Serverless ワークグループが VPC 経由でネットワークトラフィックをルーティングするかどうかを確認します。ワークグループで「拡張 VPC ルーティングをオンにする」が無効になっている場合、ルールは NON_COMPLIANT です。

識別子： REDSHIFT_SERVERLESS_WORKGROUP_ROUTES_WITHIN_VPC

リソースタイプ： AWS::RedshiftServerless::Workgroup

トリガータイプ: 定期的

AWS リージョン： 欧州 (ストックホルム) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) 、欧州 (スペイン) 、欧州 (チューリッヒ) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

redshift-unrestricted-port-access

Amazon Redshift クラスターに関連付けられたセキュリティグループに、無制限の受信トラフィックを許可するインバウンドルールがあるかどうかを確認します。Redshift クラスターポートに無制限の受信トラフィックを許可するインバウンドルールがある場合、ルールは NON_COMPLIANT です。

識別子: REDSHIFT_UNRESTRICTED_PORT_ACCESS

リソースタイプ: AWS::Redshift::Cluster

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

required-tags

指定したタグがリソースにあるかどうかを確認します。例えば、Amazon EC2 インスタンスに `CostCenter` タグがあるかどうかを確認するとともに、すべての RDS インスタンスに 1 セットの Keys タグがあるかどうかを確認できます。複数の値はカンマで区切ります。一度に確認できるタグは 6 つまでです。

AWSマネージド AWS Systems Manager オートメーションドキュメント`AWS-SetRequiredTags`は、このルールでの修復としては機能しません。修復のために、独自のカスタム Systems Manager オートメーションドキュメントを作成する必要があります。

Context: タグの形式で AWS リソースにメタデータを割り当てる AWS ことができます。各タグは、リソースまたはそのリソースに保持されているデータに関する情報を保存するためのキーとオプション値で構成されるラベルです。詳細については、「タグ付け戦略の構築」を参照してください。

このルールを使用して、どのリソースに、タグと、各タグの期待値を付けるかを指定することで、希望の設定で起動されなかったアカウント内のリソースを検索できます。修正アクションを実行してタグ付けミスを修正することもできます。ただし、このルールを使用しても、不適切なタグを使用してリソースを作成することを防ぐことはできません。

> **Note**
>
> AWS Config は、すべてのリソースタイプの関連タグの記録をサポートしているわけではありません。が特定のリソースタイプの設定項目 (CI) にタグ AWS Config を記録するかどうかを確認するには：
>
> - タグを除き、 がリソースの現在の設定 AWS Config を正しく記録していることを確認します。
> - リソースに変更が加えられたときに、 が記録された設定 AWS Config を更新することを確認します。

識別子: REQUIRED_TAGS

リソースタイプ: AWS::ACM::Certificate、AWS::AutoScaling::AutoScalingGroup、AWS::CloudFormation::Stack、AWS::Code

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

tag1Key, 型: 文字列, デフォルト: CostCenter

必須タグのキー。

tag1Value (オプション), タイプ: CSV

必須タグのオプションの値。複数の値はカンマで区切ります。

tag2Key (オプション), 型: 文字列

2 番目に必須のタグのキー。

tag2Value (オプション), タイプ: CSV

2 番目に必須のタグのオプションの値。複数の値はカンマで区切ります。

tag3Key (オプション), 型: 文字列

3 番目に必須のタグのキー。

tag3Value (オプション), タイプ: CSV

3 番目に必須のタグのオプションの値。複数の値はカンマで区切ります。

tag4Key (オプション), 型: 文字列

4 番目に必須のタグのキー。

tag4Value (オプション), タイプ: CSV

4 番目に必須のタグのオプションの値。複数の値はカンマで区切ります。

tag5Key (オプション), 型: 文字列

5 番目に必須のタグのキー。

tag5Value (オプション), タイプ: CSV

5 番目に必須のタグのオプションの値。複数の値はカンマで区切ります。

tag6Key (オプション), 型: 文字列

6 番目に必須のタグのキー。

tag6Value (オプション), タイプ: CSV

6 番目に必須のタグのオプションの値。複数の値はカンマで区切ります。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

restricted-common-ports

> **Important**
>
> このルールでは、ルール識別子 (RESTRICTED_INCOMING_TRAFFIC) とルール名 (制限付き共通ポート) が異なります。

使用中のセキュリティグループが、指定されたポートへの無制限の着信 Transmission Control Protocol (TCP) トラフィックを不許可にしているかどうかを確認します。以下の場合、ルールは COMPLIANT です。

- すべての TCP トラフィックへのポートアクセスがブロックされます。
- ポートアクセスは、単一の IPv4 アドレス、またはすべての IPv4 アドレス (「0.0.0.0/0」) をカバーしない CIDR 表記の IPv4 のアドレス範囲を送信元とするインバウンドルールによって、TCP トラフィックに開放されます。
- ポートアクセスは、単一の IPv6 アドレス、またはすべての IPv6 アドレス (「::/0)」) をカバーしない CIDR 表記の IPv6 のアドレス範囲を送信元とするインバウンドルールによって、TCP トラフィックに開放されます。

受信 TCP 接続の IP アドレスが指定されたポートに制限されていない場合、このルールは NON_COMPLIANT です。

識別子: RESTRICTED_INCOMING_TRAFFIC

リソースタイプ: AWS::EC2::SecurityGroup

トリガータイプ: 設定変更および定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

blockedPort1 (オプション), タイプ: int, デフォルト: 20

ブロックされた TCP ポート番号。デフォルトの 20 は、File Transfer Protocol (FTP) データ転送に対応します。

blockedPort2 (オプション), タイプ: int, デフォルト: 21

ブロックされた TCP ポート番号。デフォルトの 21 は、File Transfer Protocol (FTP) コマンド管理に対応します。

blockedPort3 (オプション), タイプ: int, デフォルト: 3389

ブロックされた TCP ポート番号。デフォルトの 3389 はリモートデスクトッププロトコル (RDP) に対応しています。

blockedPort4 (オプション), タイプ: int, デフォルト: 3306

ブロックされた TCP ポート番号。デフォルトの 3306 は MySQL プロトコルに対応しています。

blockedPort5 (オプション), タイプ: int, デフォルト: 4333

ブロックされた TCP ポート番号。デフォルトの 4333 は MySQL プロトコルに対応しています。

blockedPorts (オプション), タイプ: CSV

ブロックされた TCP ポート番号のカンマ区切りリスト。例えば、20、21、3306、3389、4333 などです。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

root-account-hardware-mfa-enabled

AWS アカウントが多要素認証 (MFA) ハードウェアデバイスを使用してルート認証情報でサインインできるかどうかを確認します。このルールは、ルート認証情報でサインインすることが許可されている仮想 MFA デバイスがあれば NON_COMPLIANT です。

> **Note**
>
> ルートユーザー認証情報のないアカウントには適用されません

このルールは、ルートユーザーの認証情報が存在しないNOT_APPLICABLE場合に を返します。
マネージドルールとグローバル IAM リソースタイプ
2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (AWS::IAM::Group、AWS::IAM::Policy、AWS::IAM::Role、および AWS::IAM::User) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降、 でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。
少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

識別子: ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

root-account-mfa-enabled

AWS アカウントのルートユーザーがコンソールサインインに多要素認証が必要かどうかを確認します。 AWS Identity and Access Management (IAM) ルートアカウントユーザーが多要素認証 (MFA) を有効にしていない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> ルートユーザー認証情報のないアカウントには適用されません
> このルールは、ルートユーザーの認証情報が存在しない`NOT_APPLICABLE`場合に を返します。
> マネージドルールとグローバル IAM リソースタイプ
> 2022 年 2 月より前にオンボードされたグローバル IAM リソースタイプ (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、および `AWS::IAM::User`) は、2022 年 2 月より前に AWS Config が利用可能な AWS リージョンでのみ AWS Config によって記録できます。これらのリソースタイプは、2022 年 2 月 AWS Config 以降に でサポートされているリージョンでは記録できません。これらのリージョンのリストについては、AWS 「リソースの記録 | グローバルリソース」を参照してください。
> 少なくとも 1 つのリージョンでグローバル IAM リソースタイプを記録する場合、グローバルリソースタイプのコンプライアンスを報告する定期ルールは、定期ルールが追加されたリージョンでグローバルリソースタイプの記録を有効にしていなくても、定期ルールが追加されたすべてのリージョンで評価を実行します。
> 不必要な評価を回避するため、グローバル IAM リソースタイプのコンプライアンスを報告する定期ルールは、サポートされているリージョンの 1 つにのみデプロイする必要があります。どのリージョンでどのマネージドルールがサポートされているかのリストについては、「リージョンの可用性別の AWS Config マネージドルールのリスト」を参照してください。

識別子: ROOT_ACCOUNT_MFA_ENABLED

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

route53-query-logging-enabled

Amazon Route 53 パブリックホストゾーンで DNS クエリログ記録が有効になっているかどうかを確認します。Amazon Route 53 パブリックホストゾーンで DNS クエリのログ記録が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: ROUTE53_QUERY_LOGGING_ENABLED

リソースタイプ: AWS::Route53::HostedZone

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3express-dir-bucket-lifecycle-rules-check

Amazon S3 Express ディレクトリバケットにライフサイクルルールが設定されているかどうかを確認します。アクティブなライフサイクル設定ルールがない場合、または設定がパラメータ値と一致しない場合、ルールは NON_COMPLIANT です。

識別子： S3EXPRESS_DIR_BUCKET_LIFECYCLE_RULES_CHECK

リソースタイプ： AWS::S3Express::DirectoryBucket

トリガータイプ: 設定変更

AWS リージョン： 欧州 (ストックホルム) 、アジアパシフィック (ムンバイ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、米国西部 (オレゴン) リージョンでのみ利用可能

パラメータ :

targetExpirationDays (オプション), タイプ: int

Amazon S3 Express ディレクトリバケットからオブジェクトが削除されてからの日数。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-access-point-in-vpc-only

Amazon S3 Access Points がインターネットからのアクセスを許可していないかどうかを確認します (NetworkOrigin は VPC)。NetworkOrigin が Internet の場合、ルールは NON_COMPLIANT です。

識別子: S3_ACCESS_POINT_IN_VPC_ONLY

リソースタイプ: AWS::S3::AccessPoint

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-access-point-public-access-blocks

Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっているかどうかを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

リソースタイプ: AWS::S3::AccessPoint

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

excludedAccessPoints (オプション), タイプ: CSV

許可されているパブリック Amazon S3 Access Points の名前のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-account-level-public-access-blocks

必要なパブリックアクセスブロック設定がアカウントレベルから設定されているかどうかを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

> **Note**
>
> このルールを使用している場合は、S3 へのパブリックアクセスのブロックが有効になっていることを確認します。ルールは変更によってトリガーされるため、S3 へのパブリックアクセスのブロックが有効になっていない限り、ルールは起動しません。S3 へのパブリックアクセスのブロックが有効になっていない場合、ルールは INSUFFICIENT_DATA を返します。

つまり、パブリックバケットがまだいくつかある可能性があります。S3 へのパブリックアクセスのブロック設定の詳細については、Amazon S3 ストレージへのパブリックアクセスのブロックを参照してください。

識別子: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

リソースタイプ: AWS::S3::AccountPublicAccessBlock

トリガータイプ: 設定変更 (現在のステータスはチェックされず、変更によって新しいイベントが生成される場合にのみ評価されます)

> **Note**
> このルールは、S3 エンドポイントが配置されている特定のリージョンの設定変更によってのみトリガーされます。他のすべてのリージョンでは、ルールは定期的にチェックされます。別のリージョンで変更が行われた場合、ルールが NON_COMPLIANT を返すまでに遅延が発生する可能性があります。

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

IgnorePublicAcls (オプション), 型: 文字列, デフォルト: True

IgnorePublicAcls の適用の有無。デフォルトは True

BlockPublicPolicy (オプション), 型: 文字列, デフォルト: True

BlockPublicPolicy の適用の有無。デフォルトは True

BlockPublicAcls (オプション), 型: 文字列, デフォルト: True

BlockPublicAcls の適用の有無。デフォルトは True

RestrictPublicBuckets (オプション), 型: 文字列, デフォルト: True

RestrictPublicBuckets の適用の有無。デフォルトは True

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-account-level-public-access-blocks-periodic

必要なパブリックアクセスブロック設定がアカウントレベルで設定されているかどうかを確認します。設定項目がパラメータ (またはデフォルト) の 1 つ以上の設定と一致しない場合、ルールは NON_COMPLIANT になります。

識別子: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

IgnorePublicAcls (オプション), 型: 文字列

IgnorePublicAcls の適用の有無。デフォルトは True

BlockPublicPolicy (オプション), 型: 文字列

BlockPublicPolicy の適用の有無。デフォルトは True

BlockPublicAcls (オプション), 型: 文字列

BlockPublicAcls の適用の有無。デフォルトは True

RestrictPublicBuckets (オプション), 型: 文字列

RestrictPublicBuckets の適用の有無。デフォルトは True

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-acl-prohibited

Amazon Simple Storage Service (Amazon S3) バケットが、アクセスコントロールリスト (ACL) 経由でのユーザー許可を許容するかどうかを確認します。Amazon S3 バケットでのユーザーアクセスに ACL が設定されている場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): S3_BUCKET_ACL_PROHIBITED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-blacklisted-actions-prohibited

Amazon Simple Storage Service (Amazon S3) バケットポリシーが、他の AWS アカウントのプリンシパルのバケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションを許可していないかどうかを確認します。例えば、ルールは、Amazon S3 バケットポリシーが、別の AWS アカウントがバケット内のオブジェクト`s3:DeleteObject`に対して`s3:GetBucket*`アクションを実行することを許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

> **Note**
>
> このルールでは、Principal プロパティ内のエンティティのみがチェックされ、ポリシーの Condition プロパティの条件は考慮されません。

Identifier: S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ハイデラバード) 、欧州 (スペイン) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

blacklistedActionPattern, タイプ: CSV

ブラックリストに登録されているアクションのパターン (例: s3:GetBucket* および s3:DeleteObject) のカンマ区切りのリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-cross-region-replication-enabled

Amazon S3 バケットに対して S3 クロスリージョンレプリケーションを有効にしたかどうかを確認します。クロスリージョンレプリケーションに対してレプリケーションルールが有効になっていない場合、ルールは NON_COMPLIANT です。

識別子: S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-default-lock-enabled

S3 バケットのロックがデフォルトで有効になっているかどうかを確認します。ロックが有効でない場合、ルールは NON_COMPLIANT です。

識別子: S3_BUCKET_DEFAULT_LOCK_ENABLED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

mode (オプション), 型: 文字列

> モード: (オプション): 有効な値 (GOVERNANCE または COMPLIANCE) を持つモードパラメータ。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-level-public-access-prohibited

S3 バケットがパブリックにアクセス可能かどうかを確認します。S3 バケットが `excludedPublicBuckets` パラメータにリストされておらず、バケットレベルの設定がパブリックに設定されている場合、ルールは NON_COMPLIANT です。

識別子: S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

excludedPublicBuckets (オプション), タイプ: CSV

許可されている既知のパブリック Amazon S3 バケット名のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-logging-enabled

S3 バケットに対してログ記録が有効になっているかどうか確認します。ログ記録が有効でない場合、ルールは NON_COMPLIANT です。

識別子: S3_BUCKET_LOGGING_ENABLED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

targetBucket (オプション), 型: 文字列

サーバーアクセスログの保存先の S3 バケット。

targetPrefix (オプション), 型: 文字列

サーバーアクセスログの保存先である S3 バケットのプレフィックス。

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、[AWS Config 「ルールを使用したリソースの評価」](#)を参照してください。このルールがプロアクティブモードで COMPLIANT を返すに

は、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "BucketName": "amzn-s3-demo-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "amzn-s3-demo-destination-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

s3-bucket-mfa-delete-enabled

Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっているかどうかを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

識別子: S3_BUCKET_MFA_DELETE_ENABLED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-policy-grantee-check

Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または VPCs によって制限されていることを確認します。バケットポリシーが存在しない場合、ルールは COMPLIANT です。

例えば、ルールの入力パラメータが `111122223333` および `444455556666` という 2 つのプリンシパルのリストで、バケットポリシーでは、`111122223333` のみがバケットにアクセスできると指定している場合、ルールは COMPLIANT です。同じ入力パラメータのときに、バケットポリシーで `111122223333` および `444455556666` がバケットにアクセスできると指定している場合も COMPLIANT です。

ただし、バケットポリシーで、`999900009999` がバケットにアクセスできると指定している場合、ルールは NON_COMPLIANT です。

> **Note**
> バケットポリシーに複数のステートメントが含まれている場合、バケットポリシーの各ステートメントはこのルールに対して評価されます。

識別子: S3_BUCKET_POLICY_GRANTEE_CHECK

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

awsPrincipals (オプション), タイプ: CSV

IAM ユーザー ARNs、IAM ロール ARNs、 AWS アカウントなどのプリンシパルのカンマ区切りリスト。完全な ARN を指定するか、部分一致を提供する必要があります。例えば、

「arn:aws:iam::*AccountID*:role/*role_name*」または「arn:aws:iam::*AccountID*:role/*」などです。指定された値がバケットポリシーで指定されたプリンシパル ARN と完全に一致しない場合、ルールは NON_COMPLIANT です。

servicePrincipals (オプション), タイプ: CSV

サービスプリンシパルのカンマ区切りリスト。例: 「cloudtrail.amazonaws.com, lambda.amazonaws.com」

federatedUsers (オプション), タイプ: CSV

Amazon Cognito、SAML ID プロバイダーなど、ウェブ ID フェデレーションの アイデンティティ プロバイダーのカンマ区切りリスト。例: 「cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider」

ipAddresses (オプション), タイプ: CSV

CIDR 形式の IP アドレスのカンマ区切りリスト。例: 「10.0.0.1, 192.168.1.0/24, 2001:db8::/32」

vpcIds (オプション), タイプ: CSV

Amazon Virtual Private Cloud (Amazon VPC) ID のカンマ区切りリスト。例: 「vpc-1234abc0, vpc-ab1234c0」

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-policy-not-more-permissive

Amazon Simple Storage Service バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。

> **Note**
>
> 無効なパラメータ値を指定した場合、次のエラーが表示されます。「controlPolicy パラメータの値は Amazon S3 バケットポリシーである必要があります。」

識別子: S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

controlPolicy, 型: 文字列

S3 バケットのアクセス許可の上限値を定義する Amazon S3 バケットのポリシー。ポリシーには最大 1024 文字を含めることができます。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-public-read-prohibited

Amazon S3 バケットでパブリック読み取りアクセスが許可されていないかどうかを確認します。このルールは、パブリックアクセスのブロック設定、バケットポリシー、およびバケットアクセスコントロールリスト (ACL) を確認します。

次の両方に該当するときはこのルールに準拠しています。

- Block Public Access 設定では、パブリックポリシーが制限されるか、またはバケットポリシーでパブリックの読み取りアクセスが許可されません。
- Block Public Access 設定では、パブリックの ACL が制限されるか、または ACL でパブリックの読み取りアクセスが許可されません。

このルールは次の場合に準拠されません。

- パブリックアクセスブロック設定がパブリックポリシーを制限しない場合、 AWS Config はポリシーがパブリック読み取りアクセスを許可するかどうかを評価します。ポリシーがパブリックの読み取りアクセスを許可している場合、このルールは準拠していません。

- Block Public Access 設定がパブリックバケット ACLs を制限しない場合、 AWS Config はバケット ACL がパブリック読み取りアクセスを許可するかどうかを評価します。バケット ACL でパブリック読み取りアクセスが許可されている場合、ルールは非準拠です。

> **Note**
>
> 非パブリックと見なされるには、S3 バケットポリシーが固定値へのアクセスのみを許可する必要があります。つまり、ワイルドカードまたは次の IAM ポリシー要素を含まない値です: 変数。

識別子: S3_BUCKET_PUBLIC_READ_PROHIBITED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更および定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

s3-bucket-public-write-prohibited

Amazon S3 バケットでパブリック書き込みアクセスが許可されていないかどうかを確認します。このルールは、パブリックアクセスのブロック設定、バケットポリシー、およびバケットアクセスコントロールリスト (ACL) を確認します。

次の両方に該当するときはこのルールに準拠しています。

- Block Public Access 設定でパブリックポリシーが制限されているか、またはバケットポリシーでパブリックの書き込みアクセスが許可されません。

- Block Public Access 設定でパブリック ACL が制限されているか、またはバケット ACL でパブリックの書き込みアクセスが許可されません。

このルールは次の場合に準拠されません。

- パブリックアクセスブロック設定でパブリックポリシーが制限されていない場合、 AWS Config はポリシーがパブリック書き込みアクセスを許可するかどうかを評価します。ポリシーでパブリックの書き込みアクセスが許可されている場合、このルールは非準拠です。
- Block Public Access 設定がパブリックバケット ACLs を制限しない場合、 AWS Config はバケット ACL がパブリック書き込みアクセスを許可するかどうかを評価します。バケット ACL でパブリックの書き込みアクセスが許可されている場合、このルールは非準拠です。

> **Note**
>
> このルールは、アカウントレベルのパブリックブロックアクセスに対する変更を評価しません。必要なパブリックアクセスブロックの設定がアカウントレベルから設定されているかどうかを確認するには、「s3-account-level-public-access-blocks」および「s3-account-level-public-access-blocks-periodic」を参照してください。

> **Note**
>
> 非パブリックと見なされるには、S3 バケットポリシーが固定値へのアクセスのみを許可する必要があります。つまり、ワイルドカードまたは次の IAM ポリシー要素を含まない値です: 変数。

識別子: S3_BUCKET_PUBLIC_WRITE_PROHIBITED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更および定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-replication-enabled

S3 バケットでレプリケーションルールが有効になっているかどうかを確認します。S3 バケットにレプリケーションルールがない、または有効化されていない場合、ルールは NON_COMPLIANT です。

識別子: S3_BUCKET_REPLICATION_ENABLED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ :

レプリケーションタイプ (オプション), タイプ: 文字列

> 指定できる値は、「CROSS-REGION」と「SAME-REGION」です。ルールに「CROSS-REGION」と入力して、すべてのバケットで Cross-Region レプリケーションのみが有効になっていることを確認します。ルールに「SAME-REGION」と入力して、すべてのバケットで Same-Region レプリケーションのみが有効になっていることを確認します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-server-side-encryption-enabled

Amazon S3 バケットで S3 のデフォルトの暗号化が有効になっていること、または S3 バケットポリシーが AES-256 または `put-object` を使用するサーバー側の暗号化を使用していない AWS Key Management Serviceリクエストを明示的に拒否することを確認します。Amazon S3 バケットが、デフォルトで暗号化されていない場合、ルールは NON_COMPLIANT です。

識別子: S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： 欧州 (スペイン) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-ssl-requests-only

S3 バケットに、SSL/TLS を使用するリクエストを要求するポリシーがあるかどうか確認します。いずれかの S3 バケットに HTTP リクエストを許可するポリシーがある場合、ルールは NON_COMPLIANT です。

識別子: S3_BUCKET_SSL_REQUESTS_ONLY

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-tagged

Amazon S3 バケットにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： S3_BUCKET_TAGGED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-bucket-versioning-enabled

S3 バケットに対してバージョニングが有効になっているかどうかを確認します。オプションで、S3 バケットに対して MFA 削除が有効になっているかどうかを確認します。

識別子: S3_BUCKET_VERSIONING_ENABLED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

isMfaDeleteEnabled (オプション), 型: 文字列

S3 バケットに対して MFA 削除が有効になっています。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-default-encryption-kms

S3 バケットが AWS Key Management Service (AWS KMS) で暗号化されているかどうかを確認します。S3 バケットが KMS キーで暗号化されていない場合、ルールは NON_COMPLIANT AWS です。

識別子: S3_DEFAULT_ENCRYPTION_KMS

リソースタイプ: AWS::S3::バケット、AWS::KMS::Key

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

kmsKeyArns (オプション), タイプ: CSV

Amazon S3 AWS バケットの暗号化に使用できる KMS キー ARNs のカンマ区切りリスト。Amazon S3

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-event-notifications-enabled

S3 バケットで Amazon S3 イベント通知が有効になっているかどうかを確認します。S3 イベント通知がバケットに設定されていない場合、またはイベントタイプまたは宛先が `eventTypes` および destinationArn パラメータと一致しない場合、ルールは NON_COMPLIANT になります。

識別子: S3_EVENT_NOTIFICATIONS_ENABLED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

destinationArn (オプション), タイプ: 文字列

イベント通知の送信先の Amazon リソースネーム (ARN) (Amazon SNS トピック、 AWS Lambda、Amazon SQS キュー) 。

eventTypes (オプション), タイプ: CSV

優先された Amazon S3 イベントタイプのカンマ区切りリスト

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-last-backup-recovery-point-created

Amazon Simple Storage Service (Amazon S3) のリカバリポイントが作成されたかどうかを確認します。Amazon S3 バケットに対応するリカバリポイントが指定した期間内に作成されていない場合、ルールは NON_COMPLIANT です。

識別子: S3_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon S3 バケットのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon S3 バケットの名前。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-lifecycle-policy-check

Amazon Simple Storage Service (Amazon S3) バケットのライフサイクルルールが設定されているかどうかを確認します。アクティブなライフサイクル設定ルールがない場合、または設定がパラメータ値と一致しない場合、ルールは NON_COMPLIANT です。

識別子: S3_LIFECYCLE_POLICY_CHECK

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

targetTransitionDays (オプション), タイプ: int

オブジェクトが、その作成後、指定されたストレージクラスに移行するまでの日数 (例: 30 日)。

targetExpirationDays (オプション), タイプ: int

オブジェクトが作成されてから削除されるまでの日数 (例: 395 日)。

targetTransitionStorageClass (オプション), タイプ: 文字列

送信先ストレージクラスタイプ。例えば、Amazon S3 Standard-Infrequent Access (S3 Standard-IA) などです。詳細については、Amazon S3ストレージクラスの理解と管理」を参照してください。

targetPrefix (オプション), 型: 文字列

1 つ以上のオブジェクトを識別するための Amazon S3 オブジェクトプレフィックス。

bucketNames (オプション), タイプ: CSV

ライフサイクルポリシーが有効化されている Amazon S3 バケット名のカンマ区切りのリストです。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

s3-meets-restore-time-target

Amazon Simple Storage Service (Amazon S3) バケットの復元時間が、指定された期間と一致しているかどうかを確認します。Amazon S3 バケットの LatestRestoreExecutionTimeMinutes が maxRestoreTime の値より大きい場合、ルールは NON_COMPLIANT です。

識別子: S3_MEETS_RESTORE_TIME_TARGET

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) の各 AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

maxRestoreTime, タイプ: int

最大許容復元ランタイムの数値。

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon S3 バケットのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon S3 バケットの名前。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-resources-in-logically-air-gapped-vault

Amazon Simple Storage Service (Amazon S3) バケットが論理エアギャップボールトにあるかどうかを確認します。Amazon S3 バケットが指定された期間内に論理エアギャップボールトにない場合、ルールは NON_COMPLIANT です。

識別子: S3_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 定期的

AWS リージョン： 欧州 (ストックホルム) 、中東 (バーレーン) 、アジアパシフィック (ムンバイ) 、欧州 (パリ) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、アジアパシフィック

(大阪) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、米国西部 (北カリフォルニア) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) リージョンでのみご利用いただけます。

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon S3 バケットのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon S3 バケットの名前。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 2184 以下、日は 91 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-resources-protected-by-backup-plan

Amazon Simple Storage Service (Amazon S3) バケットがバックアッププランで保護されているかどうかを確認します。Amazon S3 バケットがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

識別子: S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Amazon S3 バケットのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

チェックするルールの Amazon S3 バケットの名前。

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

s3-version-lifecycle-policy-check

Amazon Simple Storage Service (Amazon S3) のバージョニングが有効化されたバケットにライフサイクルポリシーが設定されているかどうかを確認します。Amazon S3 ライフサイクルポリシーが有効化されていない場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): S3_VERSION_LIFECYCLE_POLICY_CHECK

リソースタイプ: AWS::S3::Bucket

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

bucketNames (オプション), タイプ: CSV

ライフサイクルポリシーが有効化されている Amazon S3 バケット名のカンマ区切りのリストです。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-app-image-config-tagged

Amazon SageMaker アプリイメージ設定にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： SAGEMAKER_APP_IMAGE_CONFIG_TAGGED

リソースタイプ： AWS::SageMaker::AppImageConfig

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-domain-in-vpc

Amazon SageMaker ドメインがEFS 以外のトラフィックに顧客所有の Amazon Virtual Private Cloud (VPC) を使用しているかどうかを確認します。configuration.AppNetworkAccessType が VpcOnly に設定されていない場合、ルールは NON_COMPLIANT です。

識別子： SAGEMAKER_DOMAIN_IN_VPC

リソースタイプ： AWS::SageMaker::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-domain-tagged

Amazon SageMaker ドメインにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： SAGEMAKER_DOMAIN_TAGGED

リソースタイプ： AWS::SageMaker::Domain

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-endpoint-configuration-kms-key-configured

Key Management Service (AWS KMS) AWS キーが Amazon SageMaker エンドポイント設定に設定されているかどうかを確認します。Amazon SageMaker エンドポイントの設定に対して 'KmsKeyId' が指定されていない場合、ルールは NON_COMPLIANT です。

識別子: SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

リソースタイプ: AWS::SageMaker::EndpointConfig

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

kmsKeyArns (オプション), タイプ: 文字列

Amazon SageMaker エンドポイント設定で許可される特定の AWS KMS キー ARNs のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-endpoint-config-prod-instance-count

Amazon SageMaker エンドポイント設定に、量産バリアント「InitialInstanceCount」が 1 より大きい値に設定されているかどうかを確認します。量産バリアント「InitialInstanceCount」が 1 に等しい場合、ルールは NON_COMPLIANT です。

識別子: SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUNT

リソースタイプ: AWS::SageMaker::EndpointConfig

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-feature-group-tagged

Amazon SageMaker 特徴量グループにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： SAGEMAKER_FEATURE_GROUP_TAGGED

リソースタイプ： AWS::SageMaker::FeatureGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-image-description

Amazon SageMaker イメージに説明があるかどうかを確認します。configuration.ImageDescription が存在しない場合、ルールは NON_COMPLIANT です。

識別子： SAGEMAKER_IMAGE_DESCRIPTION

リソースタイプ： AWS::SageMaker::Image

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-image-tagged

Amazon SageMaker イメージにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： SAGEMAKER_IMAGE_TAGGED

リソースタイプ： AWS::SageMaker::Image

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-model-in-vpc

Amazon SageMaker モデルがコンテナトラフィックに Amazon Virtual Private Cloud (Amazon VPC) を使用しているかどうかを確認します。configuration.VpcConfig が存在しない場合、ルールは NON_COMPLIANT です。

識別子： SAGEMAKER_MODEL_IN_VPC

リソースタイプ： AWS::SageMaker::Model

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-model-isolation-enabled

Amazon SageMaker モデルでネットワーク分離が有効になっているかどうかを確認します。configuration.EnableNetworkIsolation が false の場合、ルールは NON_COMPLIANT です。

識別子： SAGEMAKER_MODEL_ISOLATION_ENABLED

リソースタイプ： AWS::SageMaker::Model

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-notebook-instance-inside-vpc

Amazon SageMaker ノートブックインスタンスが VPC 内または承認されたサブネットのリスト内のどちらで起動されているのかを確認します。ノートブックインスタンスが VPC 内で起動されていない場合、またはサブネット ID がパラメータリストに含まれていない場合、ルールは NON_COMPLIANT です。

識別子: SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

リソースタイプ: AWS::SageMaker::NotebookInstance

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

subnetIds (オプション), タイプ: CSV

ノートブックインスタンスを起動できるサブネット ID のカンマ区切りリストです。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-notebook-instance-kms-key-configured

Amazon SageMaker ノートブックインスタンスに AWS Key Management Service (AWS KMS) キーが設定されているかどうかを確認します。 Amazon SageMaker SageMaker ノートブックインスタンスに対して「KmsKeyId」が指定されていない場合、ルールは NON_COMPLIANT です。

識別子: SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

リソースタイプ: AWS::SageMaker::NotebookInstance

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ：

kmsKeyArns (オプション), タイプ: 文字列

Amazon SageMaker AWS ノートブックインスタンスで許可される KMS キー ARNs のカンマ区切りリスト。 Amazon SageMaker

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-notebook-instance-platform-version

Sagemaker ノートブックインスタンスが、サポートされているプラットフォーム識別子バージョンを使用するように設定されているかどうかを確認します。ノートブックインスタンスが パラメータで指定されたサポートされているプラットフォーム識別子バージョンを使用していない場合、ルールは NON_COMPLIANT です。

識別子： SAGEMAKER_NOTEBOOK_INSTANCE_PLATFORM_VERSION

リソースタイプ: AWS::SageMaker::NotebookInstance

トリガータイプ: 定期的

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

supportedPlatformIdentifierVersions, タイプ: CSV

チェックするルールでサポートされているプラットフォーム識別子バージョンのカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-notebook-instance-root-access-check

Amazon SageMaker ノートブックインスタンスで Amazon SageMaker RootAccess 設定が有効になっているかどうかを確認します。Amazon SageMaker ノートブックインスタンスで RootAccess が「有効」に設定されている場合、ルールは NON_COMPLIANT です。

識別子: SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

リソースタイプ: AWS::SageMaker::NotebookInstance

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sagemaker-notebook-no-direct-internet-access

Amazon SageMaker ノートブックインスタンスで直接インターネットアクセスが無効になっているかどうかを確認します。SageMaker ノートブックインスタンスがインターネット対応の場合、ルールは NON_COMPLIANT です。

識別子: SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

リソースタイプ: AWS::SageMaker::NotebookInstance

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

secretsmanager-rotation-enabled-check

AWS Secrets Manager シークレットでローテーションが有効になっているかどうかを確認します。このルールでは、オプションの `maximumAllowedRotationFrequency` パラメータも確認されます。 パラメータが指定されている場合、シークレットのローテーション頻度は許可されている最大頻度と比較されます。シークレットのローテーションがスケジュールされていない場合、ルールは NON_COMPLIANT です。ローテーション頻度が maximumAllowedRotationFrequency パラメータで指定された数よりも高い場合も、ルールは NON_COMPLIANT になります。

> **Note**
>
> 最初の評価から 4 時間以内にこのルールを再評価しても結果には影響しません。

識別子: SECRETSMANAGER_ROTATION_ENABLED_CHECK

リソースタイプ: AWS::SecretsManager::Secret

トリガータイプ: 設定変更

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

maximumAllowedRotationFrequency (オプション), タイプ: int

シークレットの最大許容ローテーション頻度 (日数)。

maximumAllowedRotationFrequencyInHours (オプション), タイプ: int

シークレットの最大許容ローテーション頻度 (時間)。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

secretsmanager-scheduled-rotation-success-check

AWS Secrets Manager シークレットがローテーションスケジュールに従って正常にローテーションされたかどうかを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。

> **Note**
>
> 遅延の記録
> このルールの評価結果は、ローテーション日の欠落から最大 2 日間遅延する可能性があります。より迅速なモニタリングについては、「Secrets Manager ユーザーガイド」の「Monitor AWS Secrets Manager with Amazon CloudWatch」を参照してください。
> ローテーションなしのシークレット
> このルールは、ローテーション用に設定されていないシークレット`NOT_APPLICABLE`に対して を返します。

識別子: SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

リソースタイプ: AWS::SecretsManager::Secret

トリガータイプ: 設定変更

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

secretsmanager-secret-periodic-rotation

AWS Secrets Manager のシークレットが過去指定された日数ローテーションされているかどうかを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

識別子: SECRETSMANAGER_SECRET_PERIODIC_ROTATION

リソースタイプ: AWS::SecretsManager::Secret

トリガータイプ: 定期的

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

maxDaysSinceRotation (オプション), タイプ: int

シークレットが変更されない最大日数。デフォルト値は 90 日です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

secretsmanager-secret-unused

AWS Secrets Manager シークレットが指定された日数内にアクセスされたかどうかを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コンテキスト: 未使用のシークレットは定期的に削除することをお勧めします。使用されていないシークレットは、そのシークレットを使っていた前のユーザーがそれにアクセスして誤用する可能性があります。さらに、シークレットにアクセスするユーザーが増えるにつれて、誰かがシークレットを悪用したり、権限のないエンティティへのアクセスを許可したりする可能性が高まります。未使用のシークレットを削除することで、必要としないユーザーからのシークレットへのアクセスを取り消し、 AWS Secrets Managerの使用コストを減らすすことができます。

識別子: SECRETSMANAGER_SECRET_UNUSED

リソースタイプ: AWS::SecretsManager::Secret

トリガータイプ: 定期的

AWS リージョン： メキシコ (中部) 、アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

unusedForDays (オプション), タイプ: int

シークレットを未使用のままにできる日数。デフォルト値は 90 日です。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

secretsmanager-using-cmk

内のすべてのシークレット AWS Secrets Manager が、 AWS マネージドキー （ `aws/secretsmanager`) または () で作成されたカスタマーマネージドキーを使用して暗号化されているかどうかを確認します AWS Key Management Service AWS KMS。シークレットが、カスタマーマネージド型キーを使用して暗号化されている場合、このルールは COMPLIANT です。シークレットが `aws/secretsmanager` を使用して暗号化されている場合、このルールは COMPLIANT です。

> **Note**
> このルールでは、クロスアカウントのカスタマーマネージドキーにはアクセスできず、クロスアカウントキーが使用された場合、シークレットは NON_COMPLIANT と評価されます。

識別子: SECRETSMANAGER_USING_CMK

リソースタイプ: AWS::SecretsManager::Secret

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

kmsKeyArns (オプション), タイプ: CSV

暗号化にキーが使用されているかどうかを確認するための KMS キーの Amazon リソースネーム (ARN) のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成]。

securityhub-enabled

AWS アカウントで AWS Security Hub が有効になっているかどうかを確認します。 AWS Security Hub が有効になっていない場合、ルールは NON_COMPLIANT です。

識別子:: SECURITYHUB_ENABLED

トリガータイプ: 定期的

AWS リージョン : アジアパシフィック (台北) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成]。

security-account-information-provided

AWS アカウントの連絡先にセキュリティ連絡先情報を提供したかどうかを確認します。アカウント内のセキュリティの連絡先情報が指定されていない場合、ルールは NON_COMPLIANT です。

識別子: SECURITY_ACCOUNT_INFORMATION_PROVIDED

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

service-catalog-shared-within-organization

Organizations との統合が有効になっている場合、 AWS Service Catalog がポートフォリオを組織 (単一ユニットとして扱われる AWS アカウントのコレクション) AWS と共有しているかどうかを確認します。共有の「Type」値が「ACCOUNT」の場合、ルールは NON_COMPLIANT です。

識別子: SERVICE_CATALOG_SHARED_WITHIN_ORGANIZATION

リソースタイプ: AWS::ServiceCatalog::Portfolio

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

service-vpc-endpoint-enabled

ルールパラメータで指定されたサービスのサービスエンドポイントが Amazon Virtual Private Cloud (Amazon VPC) ごとに作成されるかどうかを確認します。サービス用に作成された Amazon VPC エンドポイントが Amazon VPC にない場合、ルールは NON_COMPLIANT です。

識別子: SERVICE_VPC_ENDPOINT_ENABLED

リソースタイプ: AWS::EC2::VPC

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

serviceName, 型: 文字列

> サービスの短縮名またはサフィックス。注意: 使用可能なサービス名または有効なサフィックスのリストを取得するには、DescribeVpcEndpointServices を使用します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ses-malware-scanning-enabled

Amazon Simple Email Service (Amazon SES) で、メッセージ受信時のマルウェアおよびスパムのスキャンが有効かどうかを確認します。マルウェアおよびスパムのスキャンが有効でない場合、ルールは NON_COMPLIANT です。

識別子: SES_MALWARE_SCANNING_ENABLED

リソースタイプ: AWS::SES::ReceiptRule

トリガータイプ: 定期的

AWS リージョン: 欧州 (アイルランド)、米国東部 (バージニア北部)、米国西部 (オレゴン) リージョンでのみ利用できます

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

shield-advanced-enabled-autorenew

AWS Shield Advanced AWS がアカウントで有効になっており、このサブスクリプションが自動的に更新されるように設定されているかどうかを確認します。Shield Advanced が有効で、自動更新が有効になっている場合、ルールは COMPLIANT です。

> **Note**
>
> の API エンドポイント AWS Shield Advanced は、米国東部 (バージニア北部) リージョンでのみ使用できます。このルールは、米国東部 (バージニア北部) リージョンでのみ実行されるようにスケジュールする必要があります。

識別子: SHIELD_ADVANCED_ENABLED_AUTORENEW

トリガータイプ: 定期的

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

shield-drt-access

Shield Response Team (SRT) がアカウントにアクセスできるかどうかを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。

識別子: SHIELD_DRT_ACCESS

トリガータイプ: 定期的

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sns-encrypted-kms

SNS トピックが AWS Key Management Service (AWS KMS) で暗号化されているかどうかを確認します。SNS トピックが KMS で暗号化されていない場合、ルールは NON_COMPLIANT AWS です。必要に応じて、確認するルールのキー ARN、エイリアス ARN 、エイリアス名、またはキー ID を指定します。

識別子: SNS_ENCRYPTED_KMS

リソースタイプ: AWS::SNS::Topic

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

kmsKeyIds (オプション), タイプ: CSV

チェックするルールの AWS KMS キー Amazon リソースネーム (ARNs)、KMS エイリアス ARNs、KMS エイリアス名、または KMS キー IDs のカンマ区切りリスト。

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

sns-topic-message-delivery-notification-enabled

エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっているかどうかを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。

識別子: SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

リソースタイプ: AWS::SNS::Topic

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべてのリージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

sns-topic-no-public-access

SNS トピックアクセスポリシーがパブリックアクセスを許可するかどうかを確認します。SNS トピックアクセスポリシーがパブリックアクセスを許可している場合、このルールは NON_COMPLIANT です。

> **Note**
> 非公開と見なされるには、SNS ポリシーが固定値へのアクセスのみを許可する必要があります。つまり、ワイルドカードまたは次の IAM ポリシー要素を含まない値です: 変数。

識別子: SNS_TOPIC_NO_PUBLIC_ACCESS

リソースタイプ: AWS::SNS::Topic

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台

北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成]。

sqs-queue-no-public-access

SQS キューアクセスポリシーでパブリックアクセスが許可されているかどうかを確認します。SQS キューアクセスポリシーでパブリックアクセスが許可されている場合、ルールは NON_COMPLIANT です。

> **Note**
> 非公開と見なされるには、SQS ポリシーが固定値へのアクセスのみを許可する必要があります。つまり、ワイルドカードまたは次の IAM ポリシー要素を含まない値です: 変数。

識別子： SQS_QUEUE_NO_PUBLIC_ACCESS

リソースタイプ： AWS::SQS::Queue

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ssm-automation-block-public-sharing

AWS Systems Manager Automation でブロックパブリック共有が有効になっているかどうかを確認します。Systems Manager Automation でパブリック共有のブロックが無効になっている場合、ルールは NON_COMPLIANT です。

識別子： SSM_AUTOMATION_BLOCK_PUBLIC_SHARING

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (ソウル) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ssm-automation-logging-enabled

AWS Systems Manager Automation で Amazon CloudWatch ログ記録が有効になっているかどうかを確認します。Systems Manager Automation で CloudWatch ログ記録が有効になっていない場合、ルールは NON_COMPLIANT を返します。

識別子： SSM_AUTOMATION_LOGGING_ENABLED

リソースタイプ: AWS::::Account

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (ソウル) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべてのリージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ssm-document-not-public

アカウントが所有する AWS Systems Manager ドキュメントがパブリックかどうかを確認します。所有者が「Self」になっている Systems Manager ドキュメントがパブリックである場合、ルールは NON_COMPLIANT です。

識別子: SSM_DOCUMENT_NOT_PUBLIC

リソースタイプ: AWS::SSM::Document

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

ssm-document-tagged

AWS Systems Manager ドキュメントにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： SSM_DOCUMENT_TAGGED

リソースタイプ: AWS::SSM::Document

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

step-functions-state-machine-logging-enabled

AWS Step Functions マシンでログ記録が有効になっているかどうかを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

識別子: STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

リソースタイプ: AWS::StepFunctions::StateMachine

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

cloudWatchLogGroupArns (オプション), タイプ: CSV

Amazon CloudWatch Logs ロググループの Amazon リソースネーム (ARN) のカンマ区切りリストです。このルールは、指定されたロググループがステートマシンのログに設定されているかどうかを確認します。

logLevel (オプション), タイプ: 文字列

ステートマシンの最小ログレベルです。有効な値には、ALL、ERROR、FATAL が含まれます。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

storagegateway-last-backup-recovery-point-created

AWS Storage Gatewayボリュームの復旧ポイントが作成されたかどうかを確認します。Storage Gateway ボリュームに対応するリカバリポイントが、指定した期間内に作成されていない場合、ルールは NON_COMPLIANT です。

識別子: STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::StorageGateway::Volume

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Storage Gateway ボリュームのタグ (JSON 形式 `{"tagkey" : "tagValue"}`)。

resourceId (オプション), 型: 文字列

チェックするルールの Storage Gateway ボリュームの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

storagegateway-resources-in-logically-air-gapped-vault

AWS Storage Gatewayボリュームが論理エアギャップボールトにあるかどうかを確認します。指定した期間内に AWS Storage Gatewayボリュームが論理エアギャップボールトにない場合、ルールは NON_COMPLIANT です。

識別子: STORAGEGATEWAY_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

リソースタイプ: AWS::StorageGateway::Volume

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエ

ル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), 型: 文字列

チェックするルールの Storage Gateway ボリュームのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

チェックするルールの Storage Gateway ボリュームの ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 2184 以下、日は 91 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

storagegateway-resources-protected-by-backup-plan

AWS Storage Gatewayボリュームがバックアッププランで保護されているかどうかを確認します。Storage Gateway ボリュームがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

識別子: STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

リソースタイプ: AWS::StorageGateway::Volume

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), タイプ: 文字列

チェックするルールの Storage Gateway ボリュームのタグ (JSON 形式)。

resourceId (オプション), 型: 文字列

チェックするルールの Storage Gateway ボリュームの ID。

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

subnet-auto-assign-public-ip-disabled

Amazon Virtual Private Cloud (Amazon VPC) サブネットにパブリック IP アドレスが割り当てられているかどうかを確認します。Amazon VPC にパブリック IP アドレスが割り当てられているサブネットがない場合、ルールは COMPLIANT です。Amazon VPC にパブリック IP アドレスが割り当てられているサブネットがある場合、ルールは NON_COMPLIANT です。

識別子: SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

リソースタイプ: AWS::EC2::Subnet

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

プロアクティブな評価

このルールをプロアクティブモードで実行する手順については、AWS Config 「ルールを使用したリソースの評価」を参照してください。このルールがプロアクティブモードで COMPLIANT を返すには、StartResourceEvaluation API のリソース設定スキーマに、文字列としてエンコードされた次の入力を含める必要があります。

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

プロアクティブ評価の詳細については、「評価モード」を参照してください。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

transfer-agreement-description

AWS Transfer Family 契約に説明があるかどうかを確認します。configuration.Description が存在しない場合、ルールは NON_COMPLIANT です。

識別子： TRANSFER_AGREEMENT_DESCRIPTION

リソースタイプ： AWS::Transfer::Agreement

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

transfer-agreement-tagged

AWS Transfer Family 契約にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： TRANSFER_AGREEMENT_TAGGED

リソースタイプ： AWS::Transfer::Agreement

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

transfer-certificate-description

AWS Transfer Family 証明書に説明があるかどうかを確認します。configuration.Description が存在しない場合、ルールは NON_COMPLIANT です。

識別子： TRANSFER_CERTIFICATE_DESCRIPTION

リソースタイプ： AWS::Transfer::Certificate

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

transfer-certificate-tagged

AWS Transfer Family 証明書にタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： TRANSFER_CERTIFICATE_TAGGED

リソースタイプ： AWS::Transfer::Certificate

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

transfer-connector-logging-enabled

AWS Transfer Family Connector が Amazon CloudWatch にログを発行するかどうかを確認します。コネクタに LoggingRole が割り当てられていない場合、ルールは NON_COMPLIANT です。

識別子： TRANSFER_CONNECTOR_LOGGING_ENABLED

リソースタイプ： AWS::Transfer::Connector

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、アジアパシフィック (タイ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

transfer-connector-tagged

AWS Transfer Family コネクタにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： TRANSFER_CONNECTOR_TAGGED

リソースタイプ： AWS::Transfer::Connector

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

requiredKeyTags (オプション) , タイプ: CSV

> チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

transfer-family-server-no-ftp

AWS Transfer Family で作成されたサーバーがエンドポイント接続に FTP を使用しているかどうかを確認します。エンドポイント接続のサーバープロトコルが FTP 対応の場合、ルールは NON_COMPLIANT です。

識別子: TRANSFER_FAMILY_SERVER_NO_FTP

リソースタイプ: AWS::Transfer::Server

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

transfer-profile-tagged

AWS Transfer Family プロファイルにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： TRANSFER_PROFILE_TAGGED

リソースタイプ： AWS::Transfer::Profile

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

transfer-workflow-description

AWS Transfer Family ワークフローに説明があるかどうかを確認します。configuration.Description が存在しないか、空の文字列である場合、ルールは NON_COMPLIANT です。

識別子： TRANSFER_WORKFLOW_DESCRIPTION

リソースタイプ： AWS::Transfer::Workflow

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

transfer-workflow-tagged

AWS Transfer Family ワークフローにタグがあるかどうかを確認します。必要に応じて、タグキーを指定できます。タグがない場合、または指定されたタグキーが存在しない場合、ルールは NON_COMPLIANT です。ルールは「aws:」で始まるタグをチェックしません。

識別子： TRANSFER_WORKFLOW_TAGGED

リソースタイプ： AWS::Transfer::Workflow

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ：

requiredKeyTags (オプション) , タイプ: CSV

チェックするルールのタグキーのカンマ区切りリスト。指定した場合、評価されたリソースにこれらのキーが含まれていない場合、ルールは NON_COMPLIANT です。タグキーでは、大文字と小文字が区別されます。「aws:」で始まるタグキーは使用できません。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

virtualmachine-last-backup-recovery-point-created

AWS Backup-Gateway VirtualMachines の復旧ポイントが作成されたかどうかを確認します。 AWS Backup-Gateway VirtualMachines に、指定された期間内に作成された対応する復旧ポイントがない場合、ルールは NON_COMPLIANT です。

識別子: VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

リソースタイプ: AWS::BackupGateway::VirtualMachine

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ：

resourceTags (オプション), タイプ: 文字列

チェックするルールの AWS Backup-Gateway VirtualMachines のタグを JSON 形式で指定します`{"tagkey" : "tagValue"}`。

resourceId (オプション), タイプ: 文字列

チェックするルールの AWS Backup-Gateway VirtualMachine の ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 744 以下、日は 31 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

virtualmachine-resources-in-logically-air-gapped-vault

AWS Backup-Gateway VirtualMachines が論理エアギャップボールトにあるかどうかを確認します。Backup AWS -Gateway VirtualMachines が指定された期間内に論理エアギャップボールトにない場合、ルールは NON_COMPLIANT です。

識別子: VIRTUALMACHINE_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

リソースタイプ: AWS::BackupGateway::VirtualMachine

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), タイプ: 文字列

チェックするルールの AWS Backup-Gateway VirtualMachines のタグを JSON 形式で指定します。

resourceId (オプション), タイプ: 文字列

チェックするルールの AWS Backup-Gateway VirtualMachine の ID。

recoveryPointAgeValue (オプション), タイプ: int, デフォルト: 1

最大許容期間の数値。時間は 2184 以下、日は 91 以下。

recoveryPointAgeUnit (オプション), 型: 文字列, デフォルト:日単位

最大許容期間のための時間の単位。受け入れられる値:[時間]、[日]

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

virtualmachine-resources-protected-by-backup-plan

AWS Backup-Gateway VirtualMachines がバックアッププランで保護されているかどうかを確認します。Backup-Gateway VirtualMachine がバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

識別子: VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

リソースタイプ: AWS::BackupGateway::VirtualMachine

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

resourceTags (オプション), タイプ: 文字列

チェックするルールの AWS Backup-Gateway VirtualMachines のタグを JSON 形式で指定します`{"tagkey" : "tagValue"}`。

resourceId (オプション), タイプ: 文字列

チェックするルールの AWS Backup-Gateway VirtualMachine の ID。

crossRegionList (オプション), 型: 文字列

クロスリージョンバックアップコピーの保存先リージョンのカンマ区切りリスト

crossAccountList (オプション), 型: 文字列

クロスアカウントバックアップコピーを保持する宛先アカウントのカンマ区切りリスト

maxRetentionDays (オプション), タイプ: int

バックアップボールトロックの最大保持期間 (日数)

minRetentionDays (オプション), タイプ: int

バックアップボールトロックの最小保持期間 (日数)

backupVaultLockCheck (オプション), 型: 文字列

受け入れられる値: 「True」または「False」。ルールで、リソースがロックされたボールトにバックアップされているかどうかをチェックするには、「True」と入力します。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

vpc-default-security-group-closed

任意の Amazon Virtual Private Cloud (Amazon VPC) のデフォルトのセキュリティグループがインバウンドまたはアウトバウンドのトラフィックを許可していないかどうかを確認します。デフォルトのセキュリティグループに 1 つ以上のインバウンドトラフィックまたはアウトバウンドトラフィックがある場合、ルールは NON_COMPLIANT です。

> **Note**
>
> が Amazon VPC 削除の一部として削除されるデフォルトのセキュリティグループなどの関連リソースの削除 AWS Config を記録するまでに遅延が生じる場合があります。その結果、

デフォルトのセキュリティグループやその他の関連リソースがすべて削除または修正されたとしても、次のアカウントのベースライン化プロセスまでルールが NON_COMPLIANT と報告される場合があります。

識別子: VPC_DEFAULT_SECURITY_GROUP_CLOSED

リソースタイプ: AWS::EC2::SecurityGroup

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

vpc-endpoint-enabled

パラメータで指定された各サービスに Amazon VPC エンドポイントがあるかどうかをチェックします。各指定サービス用に作成された VPC エンドポイントが Amazon VPC にない場合、ルールは NON_COMPLIANT です。必要に応じて、ルールがチェックする特定の VPC を指定できます。

識別子: VPC_ENDPOINT_ENABLED

リソースタイプ: AWS::EC2::VPC

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

serviceNames, タイプ: CSV

サービス名またはエンドポイントのカンマ区切りリスト。例：「access-analyzer、appconfig、cloudtrail」または「com.amazonaws.region.access-analyzer」。使用可能な名前には DescribeVpcEndpointServices を使用します。

vpcIds (オプション), タイプ: CSV

VPC エンドポイントの Amazon VPC ID のカンマ区切りリスト。指定した場合、serviceName パラメータで指定されたサービスにこれらの VPC エンドポイントのいずれかがない場合、ルールは NON_COMPLIANT になります。

scopeConfigResourceTypes (オプション) , タイプ: CSV

チェックするルールの Config AWS リソースタイプのカンマ区切りリスト。指定した場合、ルールは、少なくとも 1 つの指定されたリソースがアカウントに記録されている場合にのみコンプライアンスステータスを返します。例：「AWS::SNS::Topic」。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

vpc-flow-logs-enabled

Amazon Virtual Private Cloud (Amazon VPC) フローログがすべての Amazon VPC で見つかり、有効になっているかどうかを確認します。少なくとも 1 つの Amazon VPC でフローログが有効でない場合、ルールは NON_COMPLIANT です。

識別子: VPC_FLOW_LOGS_ENABLED

リソースタイプ: AWS::EC2::VPC

トリガータイプ: 定期的

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

trafficType (オプション), 型: 文字列

フローログの TrafficType

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

vpc-network-acl-unused-check

未使用のネットワークアクセスコントロールリスト (ネットワーク ACL) があるかどうかを確認します。各ネットワーク ACL がサブネットに関連付けられている場合、ルールは COMPLIANT です。ネットワーク ACL がサブネットに関連付けられていない場合、ルールは NON_COMPLIANT です。

識別子: VPC_NETWORK_ACL_UNUSED_CHECK

リソースタイプ: AWS::EC2::NetworkAcl

トリガータイプ: 設定変更

AWS リージョン： サポートされているすべての AWS リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

vpc-peering-dns-resolution-check

アクセプタ/リクエスタ VPC からプライベート IP への DNS 解決が有効かどうかを確認します。このルールは、アクセプタ/リクエスタ VPC からプライベート IP への DNS 解決が有効でない場合、NON_COMPLIANT になります。

識別子: VPC_PEERING_DNS_RESOLUTION_CHECK

リソースタイプ: AWS::EC2::VPCPeeringConnection

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

vpcIds (オプション), タイプ: CSV

確認する VPC ID のカンマ区切りのリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

vpc-sg-open-only-to-authorized-ports

無制限の着信トラフィックを許可するセキュリティグループ (「0.0.0.0/0」または「::/0」) が、許可されたポートでのインバウンド TCP または UDP 接続のみを許可するかどうかをチェックします。このようなセキュリティグループにルールパラメータで指定されたポートがない場合、ルールは NON_COMPLIANT になります。

> **Note**
>
> このルールは、進入ルールが IPv4='0.0.0.0/0' or IPv6='::/' に設定されている Amazon EC2 セキュリティグループを評価します。セキュリティグループにこれらの宛先の 1 つもない場合、このルールは `NOT_APPLICABLE` を返します。

識別子: VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

リソースタイプ: AWS::EC2::SecurityGroup

トリガータイプ: 設定変更および定期的

AWS リージョン： アジアパシフィック (メルボルン) AWS リージョンを除く、サポートされているすべての リージョン

パラメータ :

authorizedTcpPorts (オプション), タイプ: 文字列

0.0.0.0/0 または ::/0 へのオープンが許可されている TCP ポートのカンマ区切りリスト。範囲はダッシュで定義されます (例:「443,1020-1025」)。

authorizedUdpPorts (オプション), タイプ: 文字列

0.0.0.0/0 または ::/0 へのオープンが許可されている UDP ポートのカンマ区切りリスト。範囲はダッシュで定義されます (例:「500,1020-1025」)。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

vpc-sg-port-restriction-check

セキュリティグループが、0.0.0.0/0 または ::/0 から明示的に制限されたポートに受信トラフィックを制限するかどうかを確認します。セキュリティグループが TCP/UDP ポート 22/3389 経由またはパラメータで指定された 0.0.0.0/0 または ::/0 からの受信トラフィックを許可する場合、ルールは NON_COMPLIANT です。

識別子: VPC_SG_PORT_RESTRICTION_CHECK

リソースタイプ: AWS::EC2::SecurityGroup

トリガータイプ: 定期的

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS を除く、サポートされているすべての リージョン

パラメータ :

restrictPorts (オプション), タイプ: CSV

全 IP 範囲の受信トラフィックに対して開くべきではないポートのカンマ区切りリスト。有効なポート番号の範囲は 0～65535 です。指定しない場合、ルールはデフォルトで 22 と 3389 をチェックします。

protocolType (オプション), タイプ: 文字列

チェックするルールの送信プロトコルタイプ。有効な値には、「TCP」、「UDP」、「ALL」(大文字と小文字は区別されません) が含まれます。「ALL」に設定すると、ルールは「TCP」、「UDP」、または「ALL」(-1) プロトコルのいずれかを使用するルールをチェックします。デフォルト値は「ALL」です。

excludeExternalSecurityGroups (オプション), 型: ブール値

外部セキュリティグループの評価を除外するブールフラグ。「true」に設定すると、ルールは評価に外部セキュリティグループを含めません。それ以外の場合、値が「false」に設定されている場合、すべてのセキュリティグループが評価されます。デフォルト値は「True」です。

ipType (オプション), タイプ: 文字列

チェックするルールのインターネットプロトコル (IP) バージョン。有効な値には、「IPv4」、「IPv6」、「ALL」(大文字と小文字は区別されません) が含まれます。指定しない場合、ルールはデフォルトで「ALL」をチェックします。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

vpc-vpn-2-tunnels-up

Site AWS Site-to-SiteVPN) トンネルが UP ステータスになっているかどうかを確認します。1 つまたは両方のトンネルのステータスが DOWN の場合、ルールは NON_COMPLIANT です。

識別子: VPC_VPN_2_TUNNELS_UP

リソースタイプ: AWS::EC2::VPNConnection

トリガータイプ: 設定変更

AWS リージョン： 中東 (バーレーン) 、中国 (北京) 、アジアパシフィック (大阪) 、イスラエル (テルアビブ) 、中国 (寧夏) AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

wafv2-logging-enabled

AWS WAFv2 リージョンおよびグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっているかどうかを確認します。ログ記録が有効になっていても、ログ記録の送信先がパラメータの値と一致しない場合、ルールは NON_COMPLIANT です。

> **Note**
>
> Amazon Security Lake の例外
> このルールは、 AWS WAFV2 ウェブ ACLs の Security Lake で行われたログ記録をチェックしません。

識別子: WAFV2_LOGGING_ENABLED

リソースタイプ: AWS::WAFv2::WebACL

トリガータイプ: 定期的

AWS リージョン： アジアパシフィック (タイ) 、メキシコ (中部) 、アジアパシフィック (台北) AWS を除く、サポートされているすべての リージョン

パラメータ :

KinesisFirehoseDeliveryStreamArns (オプション), タイプ: CSV

Kinesis Firehose 配信ストリーム ARN のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

wafv2-rulegroup-logging-enabled

AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっているかどうかを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

Context: AWS WAFV2 (Web Application Firewall バージョン 2) では、一般的なウェブの悪用や脆弱性からウェブアプリケーションを保護するための AWS WAF ルールを作成できます。 AWS WAF ルールグループは、ウェブ ACL (アクセスコントロールリスト) に関連付けて、ウェブアプリケーショントラフィックに必要な動作を定義できる AWS WAF ルールのコレクションです。詳しくは、「AWS WAF デベロッパーガイド」の「AWS WAF ルール」および「ルールグループ」を参照してください。

AWS WAFV2 ルールグループで CloudWatch セキュリティメトリクスコレクションを設定することで、分散型サービス拒否 (DDoS)、SQL インジェクション、クロスサイトスクリプティング (XSS) 攻撃の成功または失敗などのセキュリティメトリクスをモニタリングできます。収集されたセキュリティメトリクスは、調査を簡素化するのに役立ちます。

> **Note**
>
> チェックする AWS Config マネージド AWS WAF ルールの AWS WAFV2 ルールグループ内にルールがない場合、 AWS Config マネージドルールは を返しますNOT_APPLICABLE。

識別子: WAFV2_RULEGROUP_LOGGING_ENABLED

リソースタイプ: AWS::WAFv2::RuleGroup

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ：

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

wafv2-rulegroup-not-empty

WAFv2 ルールグループにルールが含まれているかどうかを確認します。WAFv2 ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。

識別子: WAFV2_RULEGROUP_NOT_EMPTY

リソースタイプ: AWS::WAFv2::RuleGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、アジアパシフィック (メルボルン) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

wafv2-webacl-not-empty

WAFv2 ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれているかどうかを確認します。ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていない場合、ルールは NON_COMPLIANT です。

識別子: WAFV2_WEBACL_NOT_EMPTY

リソースタイプ: AWS::WAFv2::WebACL

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

waf-classic-logging-enabled

AWS WAF Classic Global Web Access Control List (ウェブ ACLs) でログ記録が有効になっているかどうかを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

識別子: WAF_CLASSIC_LOGGING_ENABLED

リソースタイプ: AWS::WAF::WebACL

トリガータイプ: 定期的

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

パラメータ :

KinesisFirehoseDeliveryStreamArns (オプション), タイプ: CSV

AWS WAF ログの Amazon Kinesis ストリーム ARN のカンマ区切りリスト。

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

waf-global-rulegroup-not-empty

AWS WAF Classic ルールグループにルールが含まれているかどうかを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。

識別子: WAF_GLOBAL_RULEGROUP_NOT_EMPTY

リソースタイプ: AWS::WAF::RuleGroup

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

waf-global-rule-not-empty

AWS WAF グローバルルールに条件が含まれているかどうかを確認します。WAF グローバルルール内に条件がない場合、ルールは NON_COMPLIANT です。

識別子: WAF_GLOBAL_RULE_NOT_EMPTY

リソースタイプ: AWS::WAF::Rule

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成]。

waf-global-webacl-not-empty

WAF のグローバルウェブ ACL に WAF ルールまたはルールグループが含まれているかどうかを確認します。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、ルールは NON_COMPLIANT になります。

[Identifier] (識別子): WAF_GLOBAL_WEBACL_NOT_EMPTY

リソースタイプ: AWS::WAF::WebACL

トリガータイプ: 設定変更

AWS リージョン: 米国東部 (バージニア北部) リージョンでのみ利用できます

[パラメータ:]

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成]。

waf-regional-rulegroup-not-empty

WAF のリージョンルールグループにルールが含まれているかどうかを確認します。WAF リージョンルールグループにルールがない場合、ルールは NON_COMPLIANT になります。

識別子: WAF_REGIONAL_RULEGROUP_NOT_EMPTY

リソースタイプ: AWS::WAFRegional::RuleGroup

トリガータイプ: 設定変更

AWS リージョン： 中国 (北京) 、アジアパシフィック (タイ) 、アジアパシフィック (ジャカルタ) 、中東 (アラブ首長国連邦) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (大阪) 、アジアパシフィック (マレーシア) AWS GovCloud (米国東部) AWS GovCloud (米国西部) 、メキシコ (中部) 、イスラエル (テルアビブ) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) 、欧州 (スペイン) 、中国 (寧夏) 、欧州 (チューリッヒ) の各リージョン AWS を除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

waf-regional-rule-not-empty

WAF リージョンルールに条件が含まれているかどうかを確認します。リージョンルールに少なくとも 1 つの条件が含まれている場合、このルールは COMPLIANT になります。それ以外の場合は、NON_COMPLIANT になります。

識別子: WAF_REGIONAL_RULE_NOT_EMPTY

リソースタイプ: AWS::WAFRegional::Rule

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

waf-regional-webacl-not-empty

WAF のリージョンウェブ ACL に WAF ルールまたはルールグループが含まれているかどうかを確認します。ウェブ ACL に WAF ルールまたはルールグループがない場合、ルールは NON_COMPLIANT になります。

識別子: WAF_REGIONAL_WEBACL_NOT_EMPTY

リソースタイプ: AWS::WAFRegional::WebACL

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (タイ) 、アジアパシフィック (マレーシア) 、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) 、メキシコ (中部) 、アジアパシフィック (台北) 、カナダ西部 (カルガリー) AWS の各リージョンを除く、サポートされているすべての リージョン

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

workspaces-root-volume-encryption-enabled

Amazon WorkSpace ボリュームでルートボリュームの暗号化設定が有効になっているかどうかを確認します。ルートボリュームに対して暗号化設定が有効でない場合、このルールは NON_COMPLIANT です。

識別子: WORKSPACES_ROOT_VOLUME_ENCRYPTION_ENABLED

リソースタイプ: AWS::WorkSpaces::Workspace

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、アフリカ (ケープタウン) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) 、中国 (寧夏) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してください[AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成](#)。

workspaces-user-volume-encryption-enabled

Amazon WorkSpace ボリュームでユーザーボリュームの暗号化設定が有効になっているかどうかを確認します。ユーザーボリュームに対して暗号化設定が有効でない場合、このルールは NON_COMPLIANT です。

識別子: WORKSPACES_USER_VOLUME_ENCRYPTION_ENABLED

リソースタイプ: AWS::WorkSpaces::Workspace

トリガータイプ: 設定変更

AWS リージョン： アジアパシフィック (ムンバイ) 、アフリカ (ケープタウン) 、欧州 (アイルランド) 、欧州 (フランクフルト) 、南米 (サンパウロ) 、米国東部 (バージニア北部) 、アジアパシフィック (ソウル) 、欧州 (ロンドン) 、アジアパシフィック (東京) 、米国西部 (オレゴン) 、アジアパシフィック (シンガポール) 、アジアパシフィック (シドニー) 、カナダ (中部) 、中国 (寧夏) リージョンでのみ利用可能

パラメータ :

なし

AWS CloudFormation テンプレート

AWS CloudFormation テンプレートを使用して AWS Config マネージドルールを作成するには、「」を参照してくださいAWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成。

評価モード別の AWS Config マネージドルールのリスト

AWS Config は現在、次の マネージドルールをサポートしています。これらのルールを使用する前に、「」を参照してください考慮事項。

プロアクティブな評価

プロアクティブルールは、デプロイ前のリソースに対するプロアクティブ評価モードをサポートするルールです。これにより、リージョンのアカウントにあるプロアクティブルールのセットを考慮すると、 AWS リソースを定義するためにリソースプロパティのセットが COMPLIANT か NON_COMPLIANT かを評価することができます。詳細については、「評価モード」を参照してください。

> **Note**
> プロアクティブルールは、NON_COMPLIANT のフラグが付けられたリソースを修正したり、これらのリソースのデプロイを妨げたりしません。

プロアクティブな評価

- api-gw-xray-enabled
- autoscaling-group-elb-healthcheck-required
- ec2-instance-multiple-eni-check
- eip-attached
- elasticsearch-node-to-node-encryption-check
- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-public-access-check
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- s3-bucket-logging-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled

検出評価

検出ルールは、デプロイ後のリソースに対する検出評価モードをサポートするルールです。これにより、既存のリソース構成の設定を評価できます。

> **Note**
> 現在、すべての AWS Config ルールが検出評価をサポートしています。

検出評価

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged

- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged

- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration

- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled

- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- iam-server-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged

- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access

- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets

- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check

- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version

- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description

- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled

- workspaces-user-volume-encryption-enabled

トリガータイプ別の AWS Config マネージドルールのリスト

AWS Config は現在、次の マネージドルールをサポートしています。これらのルールを使用する前に、「」を参照してください考慮事項。

設定変更

変更によってトリガーされるルールは、設定の変更に応じて が AWS Config 評価するルールです。

設定変更

- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access

- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-settings-check
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check

- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled

- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled

- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-filesystem-ct-encrypted
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-supported-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version

- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-saml-provider-tagged
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-no-policies-check
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged

- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls

- msk-unrestricted-access-check
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance

- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-postgresql-logs-to-cloudwatch
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled

- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check

- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-using-cmk
- service-catalog-shared-within-organization
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

定期的

定期的なルールは、24 時間ごとなど、指定した頻度で定期的に AWS Config 評価するルールです。

定期的

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-http-to-https-redirection-check
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target

- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-last-backup-recovery-point-created
- ec2-meets-restore-time-target
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ecr-private-image-scanning-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eks-cluster-logging-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-encryption-enabled
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-server-certificate-expiration-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- kinesis-firehose-delivery-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-automatic-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- multi-region-cloud-trail-enabled
- netfw-logging-enabled
- nlb-logging-enabled
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target

- rds-mysql-instance-encrypted-in-transit
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-sqlserver-encrypted-in-transit
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-account-level-public-access-blocks-periodic
- s3-last-backup-recovery-point-created
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- waf-classic-logging-enabled

ハイブリッド

ハイブリッドルールは、設定の変更に応じて定期的に AWS Config 評価されるルールです。

ハイブリッド

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-check
- ec2-instance-launched-with-allowed-ami
- incoming-ssh-disabled
- no-unrestricted-route-to-igw
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

リージョンの可用性別の AWS Config マネージドルールのリスト

AWS Config は現在、次の マネージドルールをサポートしています。これらのルールを使用する前に、「」を参照してください考慮事項。

米国東部 (オハイオ) リージョン

米国東部 (オハイオ)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id

- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled

- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms

- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled

- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled

- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled

- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access

- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check

- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit

- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured

- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created

- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty

米国東部 (バージニア北部) リージョン

米国東部 (バージニア北部)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc

- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check

- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update

- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public

- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged

- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault

- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description

- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled

- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- iam-server-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled

- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls

- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch

- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags

- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target

- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access

- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

US West (N. California) リージョン

米国西部 (北カリフォルニア)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled

- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged

- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース

- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached

- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled

- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest

- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch

- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

米国西部 (オレゴン) リージョン

米国西部 (オレゴン)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted

- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged

- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached

- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created

- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault

- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit

- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged

- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions

- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged

- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication

- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets

- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp

- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

アフリカ（ケープタウン）リージョン

アフリカ (ケープタウン)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description

- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled

- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check

- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged

- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access

- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled

- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan

- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing

- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

アジアパシフィック (香港) リージョン

アジアパシフィック (香港)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled

- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged

- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all

- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni

- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description

- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check

- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check

- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest

- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled

- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

アジアパシフィック (ハイデラバード) リージョン

アジアパシフィック (ハイデラバード)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled

- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged

- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan

- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

アジアパシフィック (ジャカルタ) リージョン

アジアパシフィック (ジャカルタ)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding

- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check

- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions

- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check

- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled

- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target

- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags

- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged

- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created

- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

アジアパシフィック (マレーシア) リージョン

アジアパシフィック (マレーシア)

- account-part-of-organizations
- acm-certificate-expiration-check

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled

- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

アジアパシフィック (メルボルン) リージョン

アジアパシフィック (メルボルン)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade

- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault

- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- EC2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes

- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets

- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

アジアパシフィック (ムンバイ) リージョン

アジアパシフィック (ムンバイ)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest

- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled

- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled

- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged

- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check

- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check

- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged

- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled

- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled

- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check

- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check

- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan

- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

アジアパシフィック（大阪）リージョン

アジアパシフィック (大阪)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-internal-scheme-check
- alb-listener-tagged

- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists

- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled

- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-tagged
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled

- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted

- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

アジアパシフィック (ソウル) リージョン

アジアパシフィック (ソウル)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged

- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding

- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース

- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation

- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check

- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check

- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled

- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled

- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication

- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled

- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

アジアパシフィック (シンガポール) リージョン

アジアパシフィック (シンガポール)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target

- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged

- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check

- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check

- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured

- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created

- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

アジアパシフィック (シドニー) リージョン

アジアパシフィック (シドニー)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id

- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached

- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled

- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check

- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check

- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created

- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged

- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled

- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged

- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan

- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check

- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

アジアパシフィック (台北) リージョン

アジアパシフィック (台北)

- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- cloudformation-stack-drift-detection-check
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-stopped-instance
- eip-attached
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- encrypted-volumes
- incoming-ssh-disabled

- instances-in-vpc
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-versioning-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

アジアパシフィック (タイ) リージョン

アジアパシフィック (タイ)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip

- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

アジアパシフィック (東京) リージョン

アジアパシフィック (東京)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled

- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest

- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled

- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch

- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption

- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

カナダ (中部) リージョン

カナダ (中部)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled

- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists

- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled

- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled

- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode

- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check

- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

カナダ西部 (カルガリー) リージョン

カナダ西部 (カルガリー)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- batch-scheduling-policy-tagged
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cognito-user-pool-tagged

- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-prefix-list-tagged
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ecr-repository-tagged
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check

- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled

- nlb-internal-scheme-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-tagged
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

中国 (北京) リージョン

中国 (北京)

- access-keys-rotated
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- athena-workgroup-logging-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codebuild-report-group-encrypted-at-rest
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only

- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

中国 (寧夏) リージョン

中国 (寧夏)

- access-keys-rotated

- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled

- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan

- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- glue-job-logging-enabled
- glue-spark-job-supported-version
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access

- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch

- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check

- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

欧州 (フランクフルト) リージョン

欧州 (フランクフルト)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id

- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit

- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged

- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created

- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached

- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault

- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit

- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged

- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled

- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled

- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check

- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check

- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

欧州 (アイルランド) リージョン

欧州 (アイルランド)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding

- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged

- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled

- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled

- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists

- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings

- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged

- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き

- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable

- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged

- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled

- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

欧州 (ロンドン) リージョン

欧州 (ロンドン)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description

- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled

- apprunner-service-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化

- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled

- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled

- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc

- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled

- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check

- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan

- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check

- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

欧州 (ミラノ) リージョン

欧州 (ミラノ)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check

- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged

- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース

- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged

- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description

- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs

- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw

- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured

- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created

- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty

欧州 (パリ) リージョン

欧州 (パリ)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled

- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化

- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check

- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault

- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged

- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check

- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest

- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch

- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged

- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧州 (スペイン) リージョン

欧州 (スペイン)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled

- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged

- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check

- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled

- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged

- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged

- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧州 (ストックホルム) リージョン

欧州 (ストックホルム)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description

- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on

- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault

- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user

- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check

- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged

- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled

- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-バケットタグ付き
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest

- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch

- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags

- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault

- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access

- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧州 (チューリッヒ) リージョン

欧州 (チューリッヒ)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged

- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged

- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check

- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted

- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged

- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

イスラエル (テルアビブ) リージョン

イスラエル (テルアビブ)

- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged

- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-logging
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged

- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-mount-target-public-accessible
- eip-attached
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- macie-auto-sensitive-data-discovery-check
- mariadb-publish-logs-to-cloudwatch-logs
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged

- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

メキシコ (中部) リージョン

メキシコ (中部)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required

- autoscaling-launch-config-public-ip-disabled
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami

- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only

- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags

- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

中東 (バーレーン) リージョン

中東 (バーレーン)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest

- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured

- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled

- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions

- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check

- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created

- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled

- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

中東 (アラブ首長国連邦) リージョン

中東 (アラブ首長国連邦)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged

- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default

- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled

- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs

- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled

- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty

南米 (サンパウロ) リージョン

南米 (サンパウロ)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest

- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された aurora リソース
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged

- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check

- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled

- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- EC2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged

- ec2-resources-in-logically-air-gapped-vault
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- EC2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists

- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions

- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check

- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged

- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan

- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled

- workspaces-user-volume-encryption-enabled

AWS GovCloud (米国東部) リージョン

AWS GovCloud (米国東部)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-mysql-cluster-audit-logging
- バックアップ計画によって保護された aurora リソース
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック

- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-mount-target-public-accessible
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- fsx-last-backup-recovery-point-created
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-spark-job-supported-version
- guardduty-eks-protection-audit-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled

- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-cloudwatch-audit-log-enabled
- msk-cluster-public-access-disabled
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

AWS GovCloud (米国西部) リージョン

AWS GovCloud (米国西部)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-mysql-cluster-audit-logging
- バックアップ計画によって保護された aurora リソース

- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- バックアップ計画-分-頻度と分保持チェック
- バックアップ/リカバリ・ポイント暗号化
- バックアップ/リカバリ・ポイントの手動削除/無効化
- バックアップ/リカバリ・ポイントの最小保存期間チェック
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled

- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- connect-instance-logging-enabled
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-バックアップ計画によって保護されるリソース
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- バックアップ計画によって保護された EBS リソース
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled

- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- EC2-バックアップ計画によって保護されるリソース
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-public-accessible
- バックアップ計画によって保護された efs リソース
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only

- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-リソース-バックアップ計画によって保護される
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-eks-protection-audit-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check

- iam-root-access-key-check
- iam-server-certificate-expiration-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-cloudwatch-audit-log-enabled
- msk-cluster-public-access-disabled
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-バックアップ計画によって保護されるリソース
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit

- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public

- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成

> **Important**
>
> で AWS Config マネージドルールを作成するには、まず AWS Config 設定レコーダーを作成して起動する必要があります AWS CloudFormation。詳細については、「設定レコーダーの管理」を参照してください。

サポートされている AWS Config マネージドルールでは、 AWS CloudFormation テンプレートを使用してアカウントのルールを作成したり、既存の AWS CloudFormation スタックを更新したりできます。スタックとは、関連リソースの集合体のことで、ユーザーはこれを単一のユニットとしてプロビジョニングし、更新します。テンプレートを使用してスタックを起動すると、 AWS Config マネー

ジドルールが自動的に作成されます。テンプレートはルールのみを作成し、追加の AWS リソースは作成しません。

> **Note**
>
> AWS Config マネージドルールが更新されると、テンプレートが更新されて最新の変更が反映されます。ルールの特定バージョンのテンプレートを保存するには、テンプレートをダウンロードして S3 バケットにアップロードします。

AWS CloudFormation テンプレートの操作の詳細については、 AWS CloudFormation ユーザーガイドの「 の開始方法 AWS CloudFormation」を参照してください。

AWS Config マネージドルールの AWS CloudFormation スタックを起動するには

1. CloudFormation コンソールに移動し、新しいスタックを作成します。
2. [Specify template] (テンプレートを指定) の場合:
   - テンプレートをダウンロードした場合、[Upload a template file] (テンプレートファイルをアップロード) を選択し、[Choose file] (ファイルを選択) でテンプレートをアップロードします。
   - Amazon S3 URL を選択し、テンプレート URL `http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template` を入力します。

   > **Note**
   >
   > ルール識別子は ALL_CAPS_WITH_UNDERSCORES で記述する必要があります。例えば、cloudwatch-log-group-encrypted ではなく、CLOUDWATCH_LOG_GROUP_ENCRYPTED と記述します。
   > ルールによっては、ルール識別子はルール名と異なる場合があります。必ずルール識別子を使用するようにしてください。例えば、restricted-ssh のルール識別子は INCOMING_SSH_DISABLED です。

3. [Next (次へ)] を選択します。
4. スタックの詳細を指定するには、スタック名を入力し、 AWS Config ルールのパラメータ値を入力します。例えば、マネージドルールのテンプレートとして `DESIRED_INSTANCE_TYPE` を使用している場合は、「m4.large」などのインスタンスタイプを指定できます。

5. Next を選択します。
6. Options で、タグを作成したり、その他の詳細オプションを設定したりできます。これらは必須ではありません。
7. Next を選択します。
8. 確認 で、テンプレート、パラメータ、その他のオプションが正しいことを確認します。
9. Create を選択します。スタックが数分で作成されます。作成されたルールは、AWS Config コンソールで表示できます。

テンプレートを使用して、 AWS Config マネージドルールのスタックを 1 つ作成したり、アカウント内の既存のスタックを更新したりできます。スタックを削除すると、そのスタックから作成されたマネージドルールも削除されます。詳細については、AWS CloudFormation ユーザーガイドのスタックの使用を参照してください。

AWS Config カスタムルール

AWS Config カスタムルールは、ゼロから作成するルールです。 AWS Config カスタムルールを作成するには、Lambda 関数 (AWS Lambda デベロッパーガイド) とpolicy-as-code 言語である Guard (Guard GitHub リポジトリ) の 2 つの方法があります。

AWS Config Lambda で作成されたカスタムルールはAWS Config カスタム Lambda ルールと呼ばれ、Guard で作成された AWS Config カスタムルールはAWS Config カスタムポリシールールと呼ばれます。

カスタムルールを使用する前に、「」を参照してください考慮事項。

AWS Config カスタムポリシールール

Guard を使用して記述されたルールは、 AWS Config コンソールまたは AWS Config ルール APIs を使用して作成できます。 AWS Config カスタムポリシールールを使用すると、Java または Python を使用して Lambda 関数を開発し、カスタム AWS Config ルールを管理することなく、カスタムルールを作成できます。 AWS Config カスタムポリシールールは、設定の変更によって開始されます。詳細については、「Guard GitHub Repository」を参照してください。

AWS Config カスタム Lambda ルール

カスタム Lambda ルールには、Java または Python を使用して AWS Config カスタムルールの Lambda 関数を作成するオプションが用意されています。 Lambda 関数は、アップロード先のカス

タムコードであり AWS Lambda、イベントソースによって発行されるイベントによって呼び出されます。Lambda 関数が AWS Config ルールに関連付けられている場合、 AWS Config はルールの開始時にその関数を呼び出します。次に、Lambda 関数は から送信された設定情報を評価し AWS Config、評価結果を返します。Lambda 関数の詳細については、[AWS Lambda デベロッパーガイド] の [関数とイベントソース] を参照してください。

AWS Config カスタムルールの形式の違い

次の表は、ConfigurationItem データ型のフィールドと AWS Config カスタムルールのフィールドの形式の違いを示しています。

ConfigurationItem	AWS Config カスタムルール
`version`	`configurationItemVersion`
`accountId`	`awsAccountId`
`arn`	`ARN`
`configurationItemMD5Hash`	`configurationStateMd5Hash`

トピック

- AWS Config カスタムポリシールールの作成
- AWS Config カスタム Lambda ルールの作成
- AWS Config カスタム Lambda ルールにより削除されたリソースを管理する

AWS Config カスタムポリシールールの作成

AWS Config カスタムポリシールールは AWS Management Console、、 AWS CLI、または AWS Config API から作成できます。

AWS Config カスタムポリシールールの追加

Using the console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。

2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートする AWS リージョンに設定されていることを確認します。サポートされているリージョンのリストについては、「Amazon Web Services 全般のリファレンス」の「AWS Config のリージョンとエンドポイント」を参照してください。
3. 左のナビゲーションで、ルール を選択します。
4. [Rules] (ルール) ページで、A[dd rule] (ルールの追加) を選択します。
5. [Specify rule type] (ルールタイプの指定) ページで [Create custom rule using Guard] (Guard を使用したカスタムルールの作成) を選択します。
6. [ルールの設定] ページで、以下のステップを完了してルールを作成します。
   a. [Rule name] (ルール名) に、ルールの一意の名前を入力します。
   b. [説明] に、ルールの説明を入力します。
   c. Guard ランタイムバージョンでは、 AWS Config カスタムポリシールールのランタイムシステムを選択します。
   d. [Rule Content] (ルールコンテンツ) は、ルールの Guard カスタムポリシーで入力できます。
   e. 評価モードでは、リソースの作成および管理プロセスでリソース AWS Config を評価するタイミングを選択します。ルールに応じて、 はリソースのプロビジョニング前、リソースのプロビジョニング後、またはその両方でリソース設定を評価 AWS Config できます。
      i. [Turn on proactive evaluation] (プロアクティブ評価をオンにする) を選択すると、リソースをデプロイする前に、その構成設定に対して評価を実行できます。

         プロアクティブ評価をオンにした後、StartResourceEvaluation API と GetResourceEvaluationSummary API を使用して、これらのコマンドで指定したリソースが、リソースのアカウントのプロアクティブルールに基づいて NON_COMPLIANT としてフラグが設定されるかどうかを確認できます。

         このコマンドの使用の詳細については、AWS Config 「ルールを使用したリソースの評価」を参照してください。プロアクティブ評価をサポートするマネージドルールのリストについては、「評価モード別の AWS Config マネージドルールのリスト」を参照してください。
      ii. 既存のリソースの構成設定を評価するには、[Turn on detective evaluation] (検出評価を有効にする) を選択します。

検出評価の場合、 AWS Config カスタムポリシールールは設定の変更によって開始されます。このオプションは事前に選択されます。

- [Resource] (リソース) – 指定したリソースタイプや、リソースタイプおよび識別子と一致するリソースが作成、変更、または削除された場合。
- [Tags] (タグ) – 指定したタグを含むリソースが作成、変更、または削除された場合。
- すべての変更 — によって記録されたリソース AWS Config が作成、変更、または削除された場合。

AWS Config は、ルールのスコープに一致するリソースへの変更を検出すると、評価を実行します。スコープを使用して評価を開始するリソースを制限できます。それ以外の場合は、プロビジョニング後のリソースに変更があったときに評価が開始されます。

f. [Parameters] (パラメータ) では、ルールにパラメータが含まれる場合、提供されたキーの値をカスタマイズできます。パラメータは、ルールに準拠しているとみなされるためにリソースが従う必要がある属性です。

7. [レビューして作成] ページで、 AWS アカウントアカウントにルールを追加する前に、編集中のすべての選択項目を確認します。
8. ルールの確認が完了したら、[ルールの追加] を選択します。

Using the AWS CLI

`put-config-rule` コマンドを使用します。

`Owner` フィールドは `CUSTOM_POLICY` になっている必要があります。 AWS Config カスタムポリシールールには、次の追加フィールドが必要です。

- `Runtime`: AWS Config カスタムポリシールールのランタイムシステム。
- `PolicyText`: AWS Config カスタムポリシールールのロジックを含むポリシー定義。
- `EnableDebugLogDelivery`: AWS Config カスタムポリシールールのデバッグログ記録を有効にするためのブール式。デフォルト値は `false` です。

Using the API Reference

PutConfigRule アクションを使用します。

Owner フィールドは CUSTOM_POLICY になっている必要があります。 AWS Config カスタムポリシールールには、次の追加フィールドが必要です。

- Runtime: AWS Config カスタムポリシールールのランタイムシステム。
- PolicyText: AWS Config カスタムポリシールールのロジックを含むポリシー定義。
- EnableDebugLogDelivery: AWS Config カスタムポリシールールのデバッグログ記録を有効にするためのブール式。デフォルト値は false です。

AWS Config カスタムポリシールールのルールコンテンツの記述

AWS Config カスタムポリシールールを使用すると、Guard AWS CloudFormation のドメイン固有の言語 (DSL) を使用してリソース設定を評価できます。このトピックでは、カスタムポリシールールを記述するためのパターンとベストプラクティスについて説明します。

Guard でルールを記述する方法の詳細については、「Guard ユーザーガイド」の「Writing Guard rules」および「Guard GitHub リポジトリAWS CloudFormation 」の「Guard 2.0 の運用モード」を参照してください。 AWS CloudFormation

基本的なルール構造

ルールを作成するには、次の基本的な形式を使用します。

```
# Basic rule format
rule <rule_name> when
    resourceType == "<AWS::Service::Resource>" {
    # Evaluation clauses
}

# Example with filtering
let resources_of_type = Resources.*[ Type == 'AWS::Service::Resource' ]
rule check_resources when %resources_of_type !empty {
    %resources_of_type.configuration.property == expected_value
}
```

主要コンポーネント

設定

リソース設定の内容が含まれます。

supplementaryConfiguration

リソース設定の追加コンテンツが含まれています。 は、特定のリソースタイプに対してこのフィールドを AWS Config 返し、設定フィールドに対して返される情報を補足します。

resourceType

AWS 評価中の リソースタイプ。

resourceId

リソースの ID (例: `sg-xxxxxx`) 。

accountId

リソースに関連付けられている 12 桁の AWS アカウント ID。

一般的なパターン

Status checks

```
let allowed_status = ['ACTIVE', 'RUNNING']
rule check_resource_status when
    resourceType == "AWS::Service::Resource" {
    configuration.status IN %allowed_status
}
```

Required properties

```
rule check_required_properties when
    resourceType == "AWS::Service::Resource" {
    configuration.propertyName exists
    configuration.propertyName is_string  # or is_list, is_struct
}
```

Query blocks

```
configuration.Properties {
    property1 exists
```

```
    property2 is_string
    property3 IN [allowed_value1, allowed_value2]
}
```

Conditional evaluation

```
when configuration.feature_enabled == true {
    configuration.feature_settings exists
    configuration.feature_settings is_struct
}
```

Custom messages

```
rule check_compliance when
    resourceType == "AWS::Service::Resource" {
    configuration.property == expected_value <<Custom error message explaining the
 requirement>>
}}
```

高度な機能

Range checks

```
rule check_numeric_limits {
    # Inclusive range (lower_limit <= value <= upper_limit)
    configuration.value IN r[minimum_value, maximum_value]

    # Exclusive range (lower_limit < value < upper_limit)
    configuration.value IN r(exclusive_min, exclusive_max)

    # Left inclusive, right exclusive (lower_limit <= value < upper_limit)
    configuration.value IN r[minimum_value, exclusive_max)

    # Left exclusive, right inclusive (lower_limit < value <= upper_limit)
    configuration.value IN r(exclusive_min, maximum_value]
}
```

Combining conditions

```
# AND conditions (implicit through new lines)
condition_1
```

```
condition_2

# OR conditions (explicit)
condition_3 OR
condition_4
```

Chaining rules

```
rule check_prerequisites {
    configuration.required_setting exists
}

rule check_details when check_prerequisites {
    configuration.required_setting == expected_value
}
```

ベストプラクティス

- 読みやすさを向上させるには、 `let`ステートメントで変数を使用します。
- 名前付きルールブロックを使用して関連チェックをグループ化します。
- わかりやすいコメントを含めます。
- 適切な演算子 (`exists`、`is_string`、) を使用します`is_list`。
- 大文字と小文字を区別しないマッチングで正規表現パターンを使用します。

例: dynamodb-pitr-enabled

次の例は、 AWS Config マネージドルール の AWS Config カスタムポリシールールバージョンのポリシー定義を示しています[dynamodb-pitr-enabled](#)。このルールは、DynamoDB テーブルでPoint-in-Timeリカバリが有効になっているかどうかを確認します。

```
# Check if DynamoDB tables have Point-in-Time Recovery enabled
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}
```

```
rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
    let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription.pointIn
    %pitr == "ENABLED" <<DynamoDB tables must have Point-in-Time Recovery enabled>>
}
```

AWS Config カスタム Lambda ルールの作成

カスタムルールを開発し、 AWS Lambda 関数 AWS Config を使用して に追加できます。

各カスタムルールを Lambda 関数に関連付けます。これには、 AWS リソースがルールに準拠しているかどうかを評価するロジックが含まれます。この関数をルールに関連付け、設定変更または定期的な間隔に応じてルールから関数を呼び出します。次に、関数はリソースがルールに準拠しているかどうかを評価し、その評価結果を に送信します AWS Config。

AWS ルール開発キット (RDK)

AWS Rule Development Kit (RDK) は、直感的で生産的なCompliance-as-Code」ワークフローをサポートするように設計されています。カスタム Lambda 関数に基づく AWS Config ルールのデプロイに関連する未分化の重労働の多くを抽象化し、効率的なdevelop-deploy-monitorの反復プロセスを提供します。

step-by-stepの手順については、AWS 「Rule Development Kit (RDK) ドキュメント」を参照してください。

AWS Config ルールの AWS Lambda 関数の例 (Node.js)

AWS Lambda は、 AWS サービスによって発行されたイベントに応答して関数を実行します。 AWS Config Custom Lambda ルールの 関数は、 によって発行されるイベントを受け取り AWS Config、その後、イベントから受け取ったデータと AWS Config API から取得したデータを使用してルールのコンプライアンスを評価します。Config ルールの関数のオペレーションは、設定変更でトリガーされる評価を実行するか、定期的にトリガーされる評価を実行するかで異なります。

AWS Lambda 関数内の一般的なパターンについては、「 AWS Lambda デベロッパーガイド」の「プログラミングモデル」を参照してください。

Example Function for Evaluations Triggered by Configuration Changes

AWS Config は、カスタムルールの範囲内にあるリソースの設定変更を検出すると、次の例のような関数を呼び出します。

AWS Config コンソールを使用して、この例のような関数に関連付けられたルールを作成する場合は、トリガータイプとして設定の変更を選択します。 AWS Config API または を使用してルール AWS CLI を作成する場合は、 `MessageType` 属性を `ConfigurationItemChangeNotification`および に設定します`OversizedConfigurationItemChangeNotification`。これらの設定により、リソースの変更の結果として が設定項目またはオーバーサイズの設定項目 AWS Config を生成するたびに、ルールをトリガーできます。

この例では、リソースを評価し、インスタンスがリソースタイプ `AWS::EC2::Instance` と一致するかどうかを確認します。 AWS Config で設定項目またはサイズが大きすぎる設定項目が生成されると、ルールがトリガーされます。

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory
 API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
```

```
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem)
 => {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
```

```
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}

// In this example, the resource is compliant if it is an instance and its type
 matches the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration,
 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
```

```
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is
 not compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

関数のオペレーション

関数はランタイムに以下のオペレーションを実行します。

1. 関数は、 が event オブジェクトをhandler関数に AWS Lambda 渡すときに実行されます。この例では、関数は、呼び出し元に情報を返すために使用するオプションの callbackパラメータを受け入れます。 AWS Lambda また、 は、関数の実行中に使用できる情報とメソッドを含む context オブジェクトを渡します。Lambda の新しいバージョンでは、コンテキストは使用されなくなりました。
2. 関数は、イベントの messageType が設定項目であるかサイズが大きすぎる設定項目であるかを確認し、その設定項目を返します。
3. ハンドラーは、isApplicable 関数を呼び出してリソースが削除されたかどうかを確認します。

   > **Note**
   >
   > 削除されたリソースをレポートするルールは、不必要なルール評価を避けるために、NOT_APPLICABLE の評価結果を返す必要があります。

4. ハンドラーは evaluateChangeNotificationCompliance関数を呼び出し、 イベントで AWS Config 発行した configurationItemおよび ruleParameters オブジェクトを渡します。

   関数は最初にリソースが EC2 インスタンスであるかどうかを評価します。リソースが EC2 インスタンスではない場合、関数はコンプライアンス値として NOT_APPLICABLE を返します。

   次に、関数は設定項目の instanceType 属性が desiredInstanceType パラメータ値と等しいかどうかを評価します。値が等しい場合、関数は COMPLIANT を返します。値が等しくない場合、関数は NON_COMPLIANT を返します。
5. ハンドラーは、 putEvaluationsRequest オブジェクトを初期化 AWS Config して評価結果を に送信する準備をします。このオブジェクトに含まれている Evaluations パラメータは、評価対象のリソースのコンプライアンス結果、リソースタイプ、および ID を識別します。putEvaluationsRequest オブジェクトには、ルールとイベントを識別するイベントの結果トークンも含まれます AWS Config。
6. ハンドラーは、 オブジェクトをconfigクライアントの putEvaluationsメソッドに渡す AWS Config ことで、評価結果を に送信します。

Example Function for Periodic Evaluations

AWS Config は、定期的な評価のために次の例のような関数を呼び出します。定期的な評価は、AWS Configでのルールの定義時に指定した間隔で発生します。

AWS Config コンソールを使用して、この例のような関数に関連付けられたルールを作成する場合は、トリガータイプとして Periodic を選択します。 AWS Config API または を使用してルール AWS CLI を作成する場合は、 `MessageType` 属性を に設定します`ScheduledNotification`。

この例では、指定したリソースの合計数が指定した最大値を超えているかどうかを確認します。

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON
 objects passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
 numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount,
 count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not
 compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
```

```
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
```

```
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource
 type.", null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count,
 callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
```

```
}
```

関数のオペレーション

関数はランタイムに以下のオペレーションを実行します。

1. 関数は、 が event オブジェクトをhandler関数に AWS Lambda 渡すときに実行されます。この例では、関数は、呼び出し元に情報を返すために使用するオプションの callbackパラメータを受け入れます。 AWS Lambda また、 は、関数の実行中に使用できる情報とメソッドを含む context オブジェクトを渡します。Lambda の新しいバージョンでは、コンテキストは使用されなくなりました。
2. 指定したタイプのリソースをカウントするために、ハンドラーは countResourceTypes 関数を呼び出し、イベントから受け取った applicableResourceType パラメータを渡します。countResourceTypes 関数は、listDiscoveredResources クライアントの config メソッドを呼び出します。クライアントは、該当するリソースの ID のリストを返します。関数は、このリストの長さに基づいて該当するリソースの数を判断し、この数をハンドラーに返します。
3. ハンドラーは、 putEvaluationsRequest オブジェクトを初期化 AWS Config して評価結果を に送信する準備をします。このオブジェクトには、コンプライアンス結果を識別する Evaluationsパラメータと、イベントで AWS アカウント 発行された が含まれます。Evaluations パラメータでは、 AWS Configでサポートされている任意のリソースタイプに結果を適用できます。putEvaluationsRequest オブジェクトには、ルールとイベントを識別するイベントの結果トークンも含まれます AWS Config。
4. putEvaluationsRequest オブジェクト内で、ハンドラーは evaluateCompliance 関数を呼び出します。この関数は、該当するリソースの数が、イベントから提供された maxCount パラメータに割り当てた最大値を超えているかどうかをテストします。リソース数が最大値を超えている場合、関数は NON_COMPLIANT を返します。リソース数が最大値を超えていない場合、関数は COMPLIANT を返します。
5. ハンドラーは、 オブジェクトをconfigクライアントの putEvaluationsメソッドに渡す AWS Config ことで、評価結果を に送信します。

AWS Config ルールの AWS Lambda 関数の例 (Python)

AWS Lambda は、 AWS サービスによって発行されたイベントに応答して関数を実行します。 AWS Config Custom Lambda ルールの 関数は、 によって発行されるイベントを受け取り AWS Config、その後、イベントから受け取ったデータと AWS Config API から取得したデータを使用してルールの

コンプライアンスを評価します。Config ルールの関数のオペレーションは、設定変更でトリガーされる評価を実行するか、定期的にトリガーされる評価を実行するかで異なります。

AWS Lambda 関数内の一般的なパターンについては、「 AWS Lambda デベロッパーガイド」の「プログラミングモデル」を参照してください。

Example Function for Evaluations Triggered by Configuration Changes

AWS Config は、カスタムルールの範囲内にあるリソースの設定変更を検出すると、次の例のような関数を呼び出します。

AWS Config コンソールを使用して、この例のような関数に関連付けられたルールを作成する場合は、トリガータイプとして設定の変更を選択します。 AWS Config API または を使用してルール AWS CLI を作成する場合は、 `MessageType` 属性を `ConfigurationItemChangeNotification`および に設定します`OversizedConfigurationItemChangeNotification`。これらの設定により、リソースの変更の結果として が設定項目またはオーバーサイズの設定項目 AWS Config を生成するたびに、ルールをトリガーできます。

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
```

```
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] =
 json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
```

```
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'],
 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
```

```
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
```

```
        ],
        ResultToken=event['resultToken'])
```

関数のオペレーション

関数はランタイムに以下のオペレーションを実行します。

1. 関数は、 が event オブジェクトをhandler関数に AWS Lambda 渡すときに実行されます。この例では、関数は、呼び出し元に情報を返すために使用するオプションの callbackパラメータを受け入れます。 AWS Lambda また、 は、関数の実行中に使用できる情報とメソッドを含む context オブジェクトを渡します。Lambda の新しいバージョンでは、コンテキストは使用されなくなりました。
2. 関数は、イベントの messageType が設定項目であるかサイズが大きすぎる設定項目であるかを確認し、その設定項目を返します。
3. ハンドラーは、isApplicable 関数を呼び出してリソースが削除されたかどうかを確認します。

   > **Note**
   >
   > 削除されたリソースをレポートするルールは、不必要なルール評価を避けるために、NOT_APPLICABLE の評価結果を返す必要があります。

4. ハンドラーは evaluateChangeNotificationCompliance関数を呼び出し、 イベントで AWS Config 発行した configurationItemおよび ruleParameters オブジェクトを渡します。

   関数は最初にリソースが EC2 インスタンスであるかどうかを評価します。リソースが EC2 インスタンスではない場合、関数はコンプライアンス値として NOT_APPLICABLE を返します。

   次に、関数は設定項目の instanceType 属性が desiredInstanceType パラメータ値と等しいかどうかを評価します。値が等しい場合、関数は COMPLIANT を返します。値が等しくない場合、関数は NON_COMPLIANT を返します。
5. ハンドラーは、 putEvaluationsRequest オブジェクトを初期化 AWS Config して評価結果を に送信する準備をします。このオブジェクトに含まれている Evaluations パラメータは、評価対象のリソースのコンプライアンス結果、リソースタイプ、および ID を識別します。putEvaluationsRequest オブジェクトには、ルールとイベントを識別するイベントの結果トークンも含まれます AWS Config。

6. ハンドラーは、 オブジェクトをconfigクライアントの putEvaluationsメソッドに渡す AWS Config ことで、評価結果を に送信します。

Example Function for Periodic Evaluations

AWS Config は、定期的な評価のために次の例のような関数を呼び出します。定期的な評価は、AWS Configでのルールの定義時に指定した間隔で発生します。

AWS Config コンソールを使用して、この例のような関数に関連付けられたルールを作成する場合は、トリガータイプとして Periodic を選択します。 AWS Config API または を使用してルール AWS CLI を作成する場合は、 MessageType 属性を に設定しますScheduledNotification。

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
```

```
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value
 to the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled
 rules.
    Keyword arguments:
```

```
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report
 on the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])
        valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
```

```
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
ResultToken=event['resultToken'])
```

関数のオペレーション

関数はランタイムに以下のオペレーションを実行します。

1. 関数は、 が event オブジェクトをhandler関数に AWS Lambda 渡すときに実行されます。この例では、関数は、呼び出し元に情報を返すために使用するオプションの callbackパラメータを受け入れます。 AWS Lambda また、 は、関数の実行中に使用できる情報とメソッドを含む context オブジェクトを渡します。Lambda の新しいバージョンでは、コンテキストは使用されなくなりました。
2. 指定したタイプのリソースをカウントするために、ハンドラーは countResourceTypes 関数を呼び出し、イベントから受け取った applicableResourceType パラメータを渡します。countResourceTypes 関数は、listDiscoveredResources クライアントの config メソッドを呼び出します。クライアントは、該当するリソースの ID のリストを返します。関数は、このリストの長さに基づいて該当するリソースの数を判断し、この数をハンドラーに返します。
3. ハンドラーは、 putEvaluationsRequest オブジェクトを初期化 AWS Config して評価結果を に送信する準備をします。このオブジェクトには、コンプライアンス結果を識別する Evaluationsパラメータと、イベントで AWS アカウント 発行された が含まれます。Evaluations パラメータでは、 AWS Configでサポートされている任意のリソースタイプに結果を適用できます。putEvaluationsRequest オブジェクトには、ルールとイベントを識別するイベントの結果トークンも含まれます AWS Config。
4. putEvaluationsRequest オブジェクト内で、ハンドラーは evaluateCompliance 関数を呼び出します。この関数は、該当するリソースの数が、イベントから提供された maxCount パラメータに割り当てた最大値を超えているかどうかをテストします。リソース数が最大値を超えている場合、関数は NON_COMPLIANT を返します。リソース数が最大値を超えていない場合、関数は COMPLIANT を返します。
5. ハンドラーは、 オブジェクトをconfigクライアントの putEvaluationsメソッドに渡す AWS Config ことで、評価結果を に送信します。

AWS Config ルールのイベント例

ルールのトリガーが発生すると、 はイベントを発行してルールの AWS Lambda 関数を AWS Config 呼び出します。次に、 はイベントを関数のハンドラに渡して関数 AWS Lambda を実行します。

Example Event for Evaluations Triggered by Configuration Changes

AWS Config は、ルールの範囲内にあるリソースの設定変更を検出すると、イベントを発行します。次のイベント例は、EC2 インスタンスの設定変更でルールがトリガーされたことを示しています。

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Example Event for Evaluations Triggered by Oversized Configuration Changes

一部のリソースの変更では、サイズが大きすぎる設定項目が生成されます。次のイベント例は、EC2 インスタンスのサイズが大きすぎる設定変更でルールがトリガーされたことを示しています。

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
```

```
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Example Event for Evaluations Triggered by Periodic Frequency

AWS Config は、指定した頻度 (24 時間ごとなど) でリソースを評価するときにイベントを発行します。次のイベント例は、定期的な間隔でルールがトリガーされたことを示しています。

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime
\":\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",
\"recordVersion\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

イベントの属性

AWS Config イベントの JSON オブジェクトには、次の属性が含まれます。

`invokingEvent`

ルールの評価をトリガーするイベント。リソースの設定変更に応じてイベントが発行される場合、この属性の値は JSON `configurationItem` または `configurationItemSummary` (サイズが大きすぎる設定項目の場合) です。設定項目は、変更 AWS Config を検出した時点のリソースの状態を表します。設定項目の例については、 の `get-resource-config-history` AWS CLI コマンドによって生成される出力を参照してください設定履歴の表示。

定期的な評価のためにイベントが発行される場合、値は JSON オブジェクトを含む文字列です。オブジェクトには、トリガーされた評価に関する情報が含まれています。

それぞれのタイプのイベントで、次の Node.js 例を示すように、関数は JSON パーサーで文字列を解析して文字列の内容を評価する必要があります。

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

評価ロジックの一部として関数が処理するキー/値ペア。 AWS Config コンソールを使用してカスタム Lambda ルールを作成するときにパラメータを定義します。`PutConfigRule` AWS Config API リクエストまたは `put-config-rule` AWS CLI コマンドの `InputParameters` 属性を使用してパラメータを定義することもできます。

パラメータの JSON コードが文字列に含まれているため、次の Node.js 例で示すように、関数は文字列を JSON パーサーで解析して文字列の内容を評価する必要があります。

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

関数が`PutEvaluations`呼び出し AWS Config で渡す必要があるトークン。

`eventLeftScope`

評価する AWS リソースがルールのスコープから削除されたかどうかを示すブール値。値が `true` の場合、関数は、`NOT_APPLICABLE` 呼び出しの `ComplianceType` 属性の値として `PutEvaluations` を渡すことで、評価を無視できることを示します。

`executionRoleArn`

が割り当てられている IAM ロールの ARN AWS Config。

`configRuleArn`

がルールに AWS Config 割り当てた ARN。

`configRuleName`

がイベント AWS Config を発行し、 関数を呼び出す原因となったルールに割り当てた名前。

`configRuleId`

がルールに AWS Config 割り当てた ID。

`accountId`

ルールを所有 AWS アカウント する の ID。

`version`

によって割り当てられたバージョン番号 AWS。が AWS Config イベントに属性を追加すると、AWS バージョンは増加します。関数に必要な属性が特定のバージョン以上のイベントにのみある場合、その関数はこの属性の値を確認できます。

AWS Config イベントの現在のバージョンは 1.0 です。

AWS Config カスタム Lambda ルールにより削除されたリソースを管理する

削除されたリソースをレポートするルールは、不必要なルール評価を避けるために、`NOT_APPLICABLE` の評価結果を返す必要があります。

リソースを削除すると、 は `ResourceDeleted`の `configurationItem`を使用して AWS Config を作成します`configurationItemStatus`。このメタデータを使用して、ルールによって削除されたリソースについてレポートされているかを確認できます。設定アイテムの詳細については、「概念 | 設定項目」を参照してください。

次のコードスニペットを含めて、削除されたリソースをチェックし、削除されたリソースについてレポート`NOT_APPLICABLE`する場合は、 AWS Config カスタム Lambda ルールの評価結果を に設定します。

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config マネージドルールと AWS Config カスタムポリシールールは、デフォルトでこの動作を処理します。
>
> Development Kit (RDK) と AWS Config Development AWS Config Kit Library (RDKlib) を使用して Python で AWS Config カスタム Lambd ルールを作成すると、インポートされた Evaluator クラスがこの動作を確認します。RDK および RDKLib でルールを記述する方法については、「RDK および RDKLib でルールを記述する」を参照してください。

サービスにリンクされた AWS Config ルール

サービスにリンクされた AWS Config ルールは、アカウントにルールを作成するために他の AWS のサービスをサポートする一意のタイプの AWS Config マネージド AWS Config ルールです。サービスにリンクされたルールは、ユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可を含めるように事前定義されています。これらのルールは、 AWS サービスがコンプライアンス検証 AWS アカウント のために で推奨する標準に似ています。

これらのサービスにリンクされた AWS Config ルールは、 AWS サービスチームによって所有されます。 AWS サービスチームは、これらのルールを に作成します AWS アカウント。これらのルールへの読み取り専用アクセス権があります。これらのルールがリンクされている AWS サービスにサブスクライブしている場合は、これらのルールを編集または削除することはできません。

サービスにリンクされたルールと AWS Command Line Interface

では AWS CLI、PutConfigRule、DeleteConfigRule、DeleteEvaluationResults APIs、次のエラーメッセージでアクセス拒否を返します。

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

サービスにリンクされたルールと AWS Config コンソール

AWS Config コンソールでは、サービスにリンクされた AWS Config ルールがルールページに表示されます。[編集] と [削除] ボタンはコンソールでグレー表示され、ルールの編集が制限されます。ルールを選択して、ルールの詳細を表示できます。

サービスにリンクされたルール、修復アクション、適合パック

適合パックのサービスにリンクされたルールに修復アクションを追加するには、適合パックテンプレート自体に修復アクションを追加し、更新されたテンプレートで適合パックを更新する必要があります。適合パックの更新については、「Deploying a Conformance Pack (Console)」、「Deploying a Conformance Pack (AWS CLI)」、「Managing Organizational Conformance Packs」を参照してください。

サービスにリンクされたルールの編集と削除

サービスにリンクされたルールを編集または削除するには、ルールを作成した AWS サービスにお問い合わせください。たとえば、 によって作成されたサービスにリンクされたルールの場合 AWS

Security Hub、AWS Security Hub 「 ユーザーガイド: セキュリティ標準を無効にする」の手順に従って、サービスにリンクされたルールを削除できます。

組織内のすべてのアカウントでの AWS Config ルールの管理

> **Important**
> 組織のルールは、API または CLI を使用する場合に限り作成できます。このオペレーションは AWS Config コンソールではサポートされていません。

AWS Config では、組織 AWS アカウント 内のすべての で AWS Config ルールを管理できます。次のようにできます：

- 組織内のすべてのアカウントで AWS Config ルールを一元的に作成、更新、削除します。
- すべてのアカウントに共通の AWS Config ルールセットをデプロイし、 AWS Config ルールを作成すべきではないアカウントを指定します。
- の 管理アカウントの APIs を使用して AWS Organizations 、基盤となる AWS Config ルールが組織のメンバーアカウントによって変更できないようにすることで、ガバナンスを適用します。

考慮事項

異なるリージョンにまたがるデプロイの場合

アカウント間でルールとコンフォーマンスパックをデプロイする API コールは、 AWS リージョン固有です。他のリージョンにルールをデプロイする場合は、組織レベルで API コールのコンテキストを別のリージョンに変更する必要があります。例えば、米国東部 (バージニア北部) にルールをデプロイするには、リージョンを米国東部 (バージニア北部) に変更し、`PutOrganizationConfigRule` を呼び出します。

組織内のアカウントの場合

新しいアカウントが組織に参加すると、ルールまたはコンフォーマンスパックはそのアカウントにデプロイされます。アカウントが組織を離脱すると、そのルールまたはコンフォーマンスパックは削除されます。

組織のルールまたはコンフォーマンスパックを組織管理者アカウントでデプロイし、委任された管理者を確立して、委任された管理者アカウントに組織のルールまたはコンフォーマンスパックを

デプロイした場合、委任された管理者アカウントから、組織のルールやコンフォーマンスパックを表示したり、組織の管理者アカウントから、委任された管理者アカウントで組織のルールやコンフォーマンスパックを表示したりすることはできません。DescribeOrganizationConfigRules および DescribeOrganizationConformancePacks API は、これらの API を呼び出すアカウント内からデプロイされた組織関連リソースのみを表示および操作できます。

組織に追加された新しいアカウントに対する再試行メカニズム

レコーダーが利用できない場合、組織の既存のルールと組織のコンフォーマンスパックのデプロイは、アカウントを組織に追加してから 7 時間のみ再試行されます。組織にアカウントを追加してから 7 時間以内にレコーダーが存在しない場合は、レコーダーを作成する必要があります。

組織管理アカウント、委任管理者、サービスにリンクされたロール

組織管理アカウントを使用していて、組織のデプロイに委任管理者を使用する場合、 AWS Config はサービスにリンクされたロール (SLR) を自動的に作成しないことに注意してください。IAM を使用して、サービスにリンクされたロール (SLR) を手動で作成する必要があります。

管理アカウントの SLR がない場合は、委任された管理者アカウントからそのアカウントにリソースをデプロイすることはできません。管理アカウントと委任管理者アカウントからメンバーアカウントに AWS Config ルールをデプロイすることはできます。詳細については、「AWS Identity and Access Management (IAM) ユーザーガイド」の「サービスにリンクされたロールの作成」を参照してください。

デプロイ

AWS Config と統合する方法については AWS Organizations、 AWS Organizations ユーザーガイドのAWS Config 「」および AWS Organizations「」を参照してください。次の APIs、 AWS Config 録画がオンになっていることを確認します。 AWS Config AWS アカウント

- PutOrganizationConfigRule で追加または更新します。 AWS
- DescribeOrganizationConfigRules は、組織 config ルールのリストを返します。
- GetOrganizationConfigRuleDetailedStatus は、特定の組織 config ルールについて、組織内の各メンバーアカウントの詳細なステータスを返します。
- GetOrganizationCustomRulePolicy は、組織の設定に関するカスタムポリシールールのロジックを含む、ポリシー定義を返します。
- DescribeOrganizationConfigRuleStatuses は、組織 config ルールのデプロイステータスを提供します。

- DeleteOrganizationConfigRule は、指定された組織 config ルールと、その組織内のすべてのメンバーアカウントの評価結果を削除します。

リージョンのサポート

AWS 組織のメンバーアカウント間で AWS Config のルールのデプロイは、次のリージョンでサポートされています。

リージョン名	リージョン	エンドポイント	プロトコル	
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
米国西部 (北カリフォルニア)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
アジアパシフィッ	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	

リージョン名	リージョン	エンドポイント	プロトコル
ク (ハイデラバード)			
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config ルールの追加

AWS Config コンソールまたは AWS SDKs を使用してルールを追加できます。

トピック

- ルールの追加 (コンソール)
- ルールの追加 (AWS SDKs)

ルールの追加 (コンソール)

[Rules] (ルール) ページの表に、ルールとその現在のコンプライアンス結果が表示されます。各ルールの結果は、 がルールに対するリソースの評価を完了するまで、評価中... です。 AWS Config 結果は、更新ボタンを使用して更新できます。が評価 AWS Config を完了すると、準拠または非準拠のルールとリソースタイプを確認できます。詳細については、「を使用した AWS リソースのコンプライアンス情報と評価結果の表示 AWS Config」を参照してください。

> **Note**
>
> 新しいルールを追加すると、 は、以前に記録されたリソースを含む、リソースインベントリ内の該当するリソース AWS Config を評価します。たとえば、`AWS::IoT::Policy`リソースを記録したが、後で記録から除外した場合、 はインベントリに初期設定項目 (CIs AWS Config を保持します。関連付けられたリソースタイプが記録から除外されると、 はこれらの CIs を更新 AWS Config しなくなりましたが、最後に記録された状態は保持され、適用可能なルールを追加すると評価されます。
> AWS Config は、リソースインベントリにないリソースを評価しません。たとえば、amplify-branch-taggedルールを追加してもリソースを記録せず、記録したことがない場合`AWS::Amplify::Branch`、 AWS Config はアカウントの AWS Amplify ブランチが準拠しているかどうかを評価できません。
> 詳細については、「を使用した AWS リソースの記録 AWS Config」を参照してください。

ルールの追加

ルールを追加するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。

2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートするリージョンに設定されていることを確認します。サポートされているリージョンのリストについては、AWS Config の「Amazon Web Services 全般のリファレンスのリージョンとエンドポイント」を参照してください。
3. 左のナビゲーションで、ルール を選択します。
4. [Rules] (ルール) ページで、A[dd rule] (ルールの追加) を選択します。
5. [Specify rule type] (ルールタイプの指定) ページで、以下のステップを完了してルールタイプを指定します。
   a. 検索フィールドに入力して、ルール名、説明、ラベルでマネージドルールのリストをフィルタリングします。例えば、EC2 と入力すると、EC2 リソースタイプを評価するルールが返されます。periodic と入力すると、定期的にトリガーされるルールが返されます。
   b. 独自のカスタムルールを作成することもできます。Lambda を使用してカスタムルールを作成するまたは Guard を使用してカスタムルールを作成するを選択し、AWS Config 「カスタム Lambda ルールの作成」またはAWS Config 「カスタムポリシールールの作成」の手順に従います。
6. [Configure rule] (ルールの設定) ページで、以下のステップを実行してルールを設定します。
   a. 名前 に、ルールの一意の名前を入力します。
   b. [説明] に、ルールの説明を入力します。
   c. 評価モードでは、リソースの作成および管理プロセスでリソース AWS Config を評価するタイミングを選択します。ルールに応じて、 はリソースのデプロイ前、リソースのデプロイ後、またはその両方でリソース設定を評価 AWS Config できます。
      i. [Turn on proactive evaluation] (プロアクティブ評価をオンにする) を選択すると、リソースをデプロイする前に、その構成設定に対して評価を実行できます。

         プロアクティブ評価をオンにした後、StartResourceEvaluation API と GetResourceEvaluationSummary API を使用して、これらのコマンドで指定したリソースが、リソースのアカウントのプロアクティブルールに基づいて NON_COMPLIANT としてフラグが設定されるかどうかを確認できます。

         このコマンドの使用の詳細については、AWS Config 「ルールを使用したリソースの評価」を参照してください。プロアクティブ評価をサポートするマネージドルールのリストについては、「評価モード別の AWS Config マネージドルールのリスト」を参照してください。

ii. 既存のリソースの構成設定を評価するには、[Turn on detective evaluation] (検出評価を有効にする) を選択します。

検出評価には、設定変更時と定期的の 2 種類のトリガーがあります。

A. ルールのトリガータイプに設定の変更が含まれている場合は、 が Lambda 関数 AWS Config を呼び出す変更の範囲に次のいずれかのオプションを指定します。

- [Resource] (リソース) – 指定したリソースタイプや、リソースタイプおよび識別子と一致するリソースが作成、変更、または削除された場合。
- [Tags] (タグ) – 指定したタグを含むリソースが作成、変更、または削除された場合。
- すべての変更 — によって記録されたリソース AWS Config が作成、変更、または削除された場合。

AWS Config は、ルールのスコープに一致するリソースへの変更を検出すると、評価を実行します。スコープを使用して評価を開始するリソースを定義できます。

B. ルールのトリガータイプに Periodic が含まれている場合は、 が Lambda 関数を AWS Config 呼び出す頻度を指定します。

d. [Parameters] (パラメータ) では、ルールにパラメータが含まれる場合、提供されたキーの値をカスタマイズできます。パラメータは、ルールに準拠しているとみなされるためにリソースが従う必要がある属性です。

7. [レビューして作成] ページで、 AWS アカウントアカウントにルールを追加する前に、編集中のすべての選択項目を確認します。ルールが正常に動作していない場合は、[Compliance] (コンプライアンス) に以下のいずれかが表示されます。

- 結果は報告されません - ルールに対してリソースが AWS Config 評価されました。ルールがスコープ内の AWS リソースに適用されなかったか、指定されたリソースが削除されたか、評価結果が削除されました。評価結果を取得するには、ルールを更新するか、スコープを変更するか、または [Re-evaluate] (再評価) を選択します。

  このメッセージは、ルールから評価結果が報告されなかった場合にも表示される場合があります。

- 範囲内にリソースがない - どの AWS リソースもルールの範囲内にないため、記録されたリソースをこのルールに対して評価 AWS Config できません。評価結果を取得するには、ルール

を編集してその範囲を変更するか、設定ページを使用して AWS Config のリソースを追加して記録します。

- [Evaluations failed] (評価が失敗しました) - 問題の原因を判断するには、ルール名を選択して詳細ページを開き、エラーメッセージを確認します

ルールの追加 (AWS SDKs)

ルールの追加

次のサンプルコードは、`PutConfigRule` を使用する方法を説明しています。

CLI

AWS CLI

AWS マネージド Config ルールを追加するには

次のコマンドは、 AWS マネージド Config ルールを追加する JSON コードを提供します。

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` は、ルール設定を含む JSON ファイルです。

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

ComplianceResourceTypes 属性の場合、この JSON コードはスコープを AWS::EC2::Instanceタイプのリソースに制限するため、Config AWS は EC2 インスタンスのみをルールに対して評価します。このルールはマネージドルールであるため、Owner 属性は AWS に設定され、SourceIdentifier 属性はルール識別子 REQUIRED_TAGS に設定されます。InputParameters 属性には、ルールに必要なタグキー、および CostCenter と Owner が指定されます。

コマンドが成功すると、 AWS Config は出力を返しません。ルール設定を確認するには、describe-config-rules コマンドを実行してルール名を指定します。

カスタマーマネージド Config ルールを追加するには

次のコマンドは、カスタマーマネージド Config ルールを追加するための JSON コードを提供します。

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

InstanceTypesAreT2micro.json は、ルール設定を含む JSON ファイルです。

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

ComplianceResourceTypes 属性の場合、この JSON コードはスコープを AWS::EC2::Instanceタイプのリソースに制限するため、Config AWS は EC2 インスタンスのみをルールに対して評価します。このルールはカスタマーマネージドルールであるため、Owner 属性は に設定されCUSTOM_LAMBDA、 SourceIdentifier 属性は AWS Lambda 関数の ARN に設定されます。SourceDetails オブジェクトは必須です。InputParameters 属性に指定されたパラメータは、Config が呼び出してルールに対してリソースを評価するときに AWS Lambda AWS 関数に渡されます。

コマンドが成功すると、 AWS Config は出力を返しません。ルール設定を確認するには、describe-config-rules コマンドを実行してルール名を指定します。

- API の詳細については、「AWS CLI コマンドリファレンス」の「PutConfigRule」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.
```

```
        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API Reference」(AWS SDK for Python (Boto3) API リファレンス) の「PutConfigRule」を参照してください。

AWS Config ルールの更新

AWS Config コンソールまたは AWS SDKsを使用してルールを更新できます。

トピック

- ルールの更新 (コンソール)
- ルールの更新 (AWS SDKs)

ルールの更新 (コンソール)

[Rules] (ルール) ページの表に、ルールとその現在のコンプライアンス結果が表示されます。がルールに対するリソースの評価 AWS Config を完了するまで、各ルールの結果は評価中... になります。結果は、更新ボタンを使用して更新できます。が評価 AWS Config を完了すると、準拠または非準拠のルールとリソースタイプを確認できます。詳細については、「を使用した AWS リソースのコンプライアンス情報と評価結果の表示 AWS Config」を参照してください。

ルールの更新

ルールを更新するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートするリージョンに設定されていることを確認します。サポートされているリージョンのリストについては、AWS Config の「Amazon Web Services 全般のリファレンスのリージョンとエンドポイント」を参照してください。
3. 左のナビゲーションで、ルール を選択します。
4. 更新するルールを選択し、[Edit rule] (ルールの編集) をクリックします。
5. 必要に応じて [Edit rule] (ルールの編集) ページの設定を変更し、ルールを変更します。
6. [保存] を選択します。

ルールの更新 (AWS SDKs)

ルールの更新

以前に追加したルールを更新している場合は、このリクエストで使用する `ConfigRule` データ型に `ConfigRuleName`、`ConfigRuleId`、または `ConfigRuleArn` でルールを指定できます。ルールを追加するときと同じ `PutConfigRule` コマンドを使用します。

次のサンプルコードは、`PutConfigRule` を使用する方法を説明しています。

CLI

AWS CLI

AWS マネージド Config ルールを追加するには

次のコマンドは、 AWS マネージド Config ルールを追加する JSON コードを提供します。

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

RequiredTagsForEC2Instances.json は、ルール設定を含む JSON ファイルです。

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

ComplianceResourceTypes 属性の場合、この JSON コードはスコープを AWS::EC2::Instanceタイプのリソースに制限するため、Config AWS は EC2 インスタンスのみをルールに対して評価します。このルールはマネージドルールであるため、Owner 属性は AWS に設定され、SourceIdentifier 属性はルール識別子 REQUIRED_TAGS に設定されます。InputParameters 属性には、ルールに必要なタグキー、および CostCenter と Owner が指定されます。

コマンドが成功すると、 AWS Config は出力を返しません。ルール設定を確認するには、describe-config-rules コマンドを実行してルール名を指定します。

カスタマーマネージド Config ルールを追加するには

次のコマンドは、カスタマーマネージド Config ルールを追加するための JSON コードを提供します。

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` は、ルール設定を含む JSON ファイルです。

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

`ComplianceResourceTypes` 属性の場合、この JSON コードはスコープを `AWS::EC2::Instance`タイプのリソースに制限するため、Config AWS は EC2 インスタンスのみをルールに対して評価します。このルールはカスタマーマネージドルールであるため、`Owner` 属性は に設定され`CUSTOM_LAMBDA`、 `SourceIdentifier` 属性は AWS Lambda 関数の ARN に設定されます。`SourceDetails` オブジェクトは必須です。`InputParameters` 属性に指定されたパラメータは、Config が呼び出してルールに対してリソースを評価するときに AWS Lambda AWS 関数に渡されます。

コマンドが成功すると、 AWS Config は出力を返しません。ルール設定を確認するには、describe-config-rules コマンドを実行してルール名を指定します。

- API の詳細については、「AWS CLI コマンドリファレンス」の「PutConfigRule」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
```

```
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API Reference」(AWS SDK for Python (Boto3) API リファレンス) の「PutConfigRule」を参照してください。

AWS Config ルールの削除

AWS Config コンソールまたは AWS SDKs を使用してルールを削除できます。

トピック

- 考慮事項
- ルールの削除 (コンソール)
- ルールの削除 (AWS SDKs)

考慮事項

推奨事項: ルールを削除する前に**`AWS::Config::ResourceCompliance`**、リソースタイプを記録から除外することを検討してください。

ルールを削除するCIs) が作成されます。 `AWS::Config::ResourceCompliance`多数のリソースタイプを評価するルールを削除すると、記録された CI の数が増加する可能性があります。

関連するコストを回避するには、ルールを削除する前に`AWS::Config::ResourceCompliance`リソースタイプの記録を無効にし、ルールが削除された後に記録を再度有効にすることができます。

ただし、ルールの削除は非同期プロセスであるため、完了までに 1 時間以上かかる場合があります。の記録が無効になっている間`AWS::Config::ResourceCompliance`、ルール評価は関連するリソースの履歴には記録されません。

ルールの削除 (コンソール)

[Rules] (ルール) ページの表に、ルールとその現在のコンプライアンス結果が表示されます。がルールに対するリソースの評価 AWS Config を完了するまで、各ルールの結果は評価中... になります。結果は、更新ボタンを使用して更新できます。が評価 AWS Config を完了すると、準拠または非準拠のルールとリソースタイプを確認できます。詳細については、「を使用した AWS リソースのコンプライアンス情報と評価結果の表示 AWS Config」を参照してください。

> **Note**
>
> AWS Config は、記録するリソースタイプのみを評価します。例えば、cloudtrail 対応ルールを追加しても CloudTrail 証跡リソースタイプを記録しない場合、 AWS Config はアカウントの証跡が準拠しているかどうかを評価できません。詳細については、「を使用した AWS リソースの記録 AWS Config」を参照してください。

ルールの削除

ルールを削除するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートするリージョンに設定されていることを確認します。サポートされているリージョンのリストについては、AWS Config の「Amazon Web Services 全般のリファレンスのリージョンとエンドポイント」を参照してください。
3. 左のナビゲーションで、ルール を選択します。
4. テーブルから削除するルールを選択します。
5. [Actions] (アクション) ドロップダウンリストから、[Delete rule] (ルールの削除) を選択します。
6. プロンプトが表示されたら、「Delete」(大文字と小文字を区別) と入力し、[Delete] (削除) をクリックします。

ルールの削除 (AWS SDKs)

ルールの削除

次のサンプルコードは、`DeleteConfigRule` を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールを削除するには

次のコマンドは、 という名前 AWS の Config ルールを削除しますMyConfigRule。

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- API の詳細については、AWS CLI コマンドリファレンスの「DeleteConfigRule」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
```

```
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API Reference」(AWS SDK for Python (Boto3) API リファレンス) の「DeleteConfigRule」を参照してください。

AWS Config ルールの詳細とコンプライアンス情報の表示

> **Important**
>
> コンプライアンスステータスを正確に報告するには、`AWS::Config::ResourceCompliance` リソースタイプを記録する必要があります。詳細については、AWS 「リソースの記録」を参照してください。

AWS Config コンソールまたは AWS SDKs を使用してルールを表示できます。

トピック

- ルールの表示 (コンソール)
- ルールの表示 (AWS SDKs)

ルールの表示 (コンソール)

[Rules] (ルール) ページの表に、ルールとその現在のコンプライアンス結果が表示されます。がルールに対するリソースの評価 AWS Config を完了するまで、各ルールの結果は評価中... です。結果は、更新ボタンを使用して更新できます。が評価 AWS Config を完了すると、準拠または非準拠のルールとリソースタイプを確認できます。詳細については、「を使用した AWS リソースのコンプライアンス情報と評価結果の表示 AWS Config」を参照してください。

> **Note**
>
> AWS Config は、記録するリソースタイプのみを評価します。例えば、cloudtrail 対応ルールを追加しても CloudTrail 証跡リソースタイプを記録しない場合、 AWS Config はアカウントの証跡が準拠しているかどうかを評価できません。詳細については、「を使用した AWS リソースの記録 AWS Config」を参照してください。

ルールの表示

ルールを表示するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートするリージョンに設定されていることを確認します。サポートされているリージョンのリストについては、AWS Config の「Amazon Web Services 全般のリファレンスのリージョンとエンドポイント」を参照してください。
3. 左のナビゲーションで、ルール を選択します。
4. ルールページには、現在 にあるすべてのルールが表示されます AWS アカウント。ここには、各ルールの名前、関連する修復アクション、およびコンプライアンスステータスが一覧表示されます。
   - [Add rule] (ルールの追加) を選択し、ルールの作成を開始します。
   - ルールを選択して設定を表示するか、ルールを選択して [View details] (詳細を表示) をクリックします。
   - リソースを評価したときのルールのコンプライアンス状態が表示されます。
   - ルールを選択し、[Edit rule] (ルールの編集) をクリックしてルールの設定を変更し、準拠していないルールの修復アクションを設定します。

ルールの表示 (AWS SDKs)

ルールの詳細の表示

次のサンプルコードは、`DescribeConfigRules` を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールの詳細を取得するには

次のコマンドは、 という名前 AWS の Config ルールの詳細を返しますInstanceTypesAreT2micro。

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

出力:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
```

```
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeConfigRules」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: このサンプルは、選択したプロパティを持つアカウントの設定ルールを一覧表示します。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

出力:

```
ConfigRuleName                                   ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                   ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                            config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                              config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required       config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V4)」のDescribeConfigRules」を参照してください。

Tools for PowerShell V5

例 1: このサンプルは、選択したプロパティを持つアカウントの設定ルールを一覧表示します。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

出力:

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                  ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                           config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                             config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required      config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V5)」のDescribeConfigRules」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
```

```
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- API の詳細については、「AWS SDK for Python (Boto3) API Reference」(AWS SDK for Python (Boto3) API リファレンス) の「DescribeConfigRules」を参照してください。

ルールのコンプライアンス情報の表示

次のサンプルコードは、`DescribeComplianceByConfigRule` を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールのコンプライアンス情報を取得するには

次のコマンドは、1 つ以上の AWS リソースによって違反された各 AWS Config ルールのコンプライアンス情報を返します。

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

出力では、各 CappedCount 属性の値は、関連するルールに準拠していないリソースの数を示します。例えば、次の出力は、3 つのリソースが InstanceTypesAreT2micro という名前のルールに準拠していないことを示しています。

出力:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeComplianceByConfigRule」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ルールの現在の評価結果がないため、INSUFFICIENT_DATA が返されるルール ebs-optimized-instance のコンプライアンスの詳細を取得します。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

出力:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

例 2: この例では、ルール ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK の非準拠リソースの数を返します。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

出力:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- API の詳細については、「 コマンドレットリファレンス (V4)」のDescribeComplianceByConfigRule」を参照してください。 AWS Tools for PowerShell

Tools for PowerShell V5

例 1: この例では、ルールの現在の評価結果がないため、INSUFFICIENT_DATA が返されるルール ebs-optimized-instance のコンプライアンスの詳細を取得します。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

出力:

```
ComplianceContributorCount ComplianceType
```

```
-------------------------- --------------
                           INSUFFICIENT_DATA
```

例 2: この例では、ルール ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK の非準拠リソースの数を返します。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

出力:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- API の詳細については、「 コマンドレットリファレンス (V5)」のDescribeComplianceByConfigRule」を参照してください。 AWS Tools for PowerShell

ルールのコンプライアンス概要の表示

次のサンプルコードは、`GetComplianceSummaryByConfigRule` を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールのコンプライアンス概要を取得するには

次のコマンドは、準拠しているルールの数と準拠していないルールの数を返します。

```
aws configservice get-compliance-summary-by-config-rule
```

出力では、各 `CappedCount` 属性の値は、準拠または非準拠のルールの数を示します。

出力:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
```

```
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetComplianceSummaryByConfigRule」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: このサンプルは、非準拠の Config ルールの数を返します。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

出力:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V4)」のGetComplianceSummaryByConfigRule」を参照してください。

Tools for PowerShell V5

例 1: このサンプルは、非準拠の Config ルールの数を返します。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

出力:

```
CapExceeded CappedCount
```

```
----------- -----------
False       9
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のGetComplianceSummaryByConfigRule」を参照してください。

ルールの評価結果の表示

次のサンプルコードは、`GetComplianceDetailsByConfigRule` を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールの評価結果を取得するには

次のコマンドは、 という名前の Config AWS ルールに準拠していないすべてのリソースの評価結果を返します`InstanceTypesAreT2micro`。

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

出力:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetComplianceDetailsByConfigRule」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ルール access-keys-rotated の評価結果を取得し、コンプライアンスタイプ別にグループ化された出力を返します。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

出力:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

例 2: この例では、COMPLIANT リソースの access-keys-rotated ルールのコンプライアンスの詳細をクエリします。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

出力:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V4)」の[GetComplianceDetailsByConfigRule](#)」を参照してください。

Tools for PowerShell V5

例 1: この例では、ルール access-keys-rotated の評価結果を取得し、コンプライアンスタイプ別にグループ化された出力を返します。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

出力:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
```

```
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

例 2: この例では、COMPLIANT リソースの access-keys-rotated ルールのコンプライアンスの詳細をクエリします。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

出力:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のGetComplianceDetailsByConfigRule」を参照してください。

AWS Config ルールのプロアクティブ評価を有効にする

AWS Config コンソールまたは AWS SDKs を使用して、プロアクティブ評価ルールを有効にできます。プロアクティブ評価をサポートするリソースタイプとマネージドルールのリストについては、「ルールのコンポーネント | 評価モード」を参照してください。

トピック

- プロアクティブな評価を有効にする (コンソール)
- プロアクティブ評価 (AWS SDKsを有効にする

プロアクティブな評価を有効にする (コンソール)

[Rules] (ルール) ページの表に、ルールとその現在のコンプライアンス結果が表示されます。各ルールの結果は、 がルールに対するリソースの評価を完了するまで、評価中... です。 AWS Config 結果は、更新ボタンを使用して更新できます。

が評価 AWS Config を完了すると、準拠または非準拠のルールとリソースタイプを確認できます。詳細については、「を使用した AWS リソースのコンプライアンス情報と評価結果の表示 AWS Config」を参照してください。

> **Note**
>
> AWS Config は、記録しているリソースタイプのみを評価します。例えば、cloudtrail 対応ルールを追加しても CloudTrail 証跡リソースタイプを記録しない場合、 AWS Config はアカウントの証跡が準拠しているかどうかを評価できません。詳細については、「を使用した AWS リソースの記録 AWS Config」を参照してください。

プロアクティブな評価を有効にする

プロアクティブ評価を使用して、デプロイ前のリソースを評価できます。これにより、リージョンのアカウントにあるプロアクティブルールのセットを考慮すると、 AWS リソースを定義するためにリソースプロパティのセットが COMPLIANT か NON_COMPLIANT かを評価することができます。

リソースタイプスキーマは、リソースのプロパティを記述します。リソースタイプスキーマは、AWS CloudFormation レジストリ内のAWS 「パブリック拡張」または次の CLI コマンドで確認できます。

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

詳細については、「 AWS CloudFormation ユーザーガイド」の AWS CloudFormation 「レジストリ、リソース、プロパティタイプのリファレンスによる拡張機能の管理」を参照してください。AWS

> **Note**
>
> プロアクティブルールは、NON_COMPLIANT のフラグが付けられたリソースを修正したり、これらのリソースのデプロイを妨げたりしません。

プロアクティブな評価を有効にするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。

2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートするリージョンに設定されていることを確認します。サポートされている AWS リージョンのリストについては、Amazon Web Services 全般のリファレンス の「AWS Config のリージョンとエンドポイント」を参照してください。
3. 左のナビゲーションで、ルール を選択します。プロアクティブ評価をサポートするマネージドルールのリストについては、「評価モード別の AWS Config マネージドルールのリスト」を参照してください。
4. ルールを選択し、更新するルールの [Edit rule] (ルールの編集) をクリックします。
5. [Evaluation mode] (評価モード) で、[Turn on proactive evaluation] (プロアクティブな評価をオンにする) を選択し、デプロイ前のリソースの構成設定に対して評価を実行します。
6. [保存] を選択します。

プロアクティブ評価をオンにした後、StartResourceEvaluation API と GetResourceEvaluationSummary API を使用して、これらのコマンドで指定したリソースが、リソースのアカウントのプロアクティブルールに基づいて NON_COMPLIANT としてフラグが設定されるかどうかを確認できます。

例えば、StartResourceEvaluation API を開始します。

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

出力に `ResourceEvaluationId` が表示されます。

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

次に、`ResourceEvaluationId` を GetResourceEvaluationSummary API で使用して評価結果を確認します。

```
aws configservice get-resource-evaluation-summary
```

```
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

次のような出力が表示されます。

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

どのルールがリソースに NON_COMPLIANT のフラグを付けたかなど、評価結果に関する詳細を確認するには、GetComplianceDetailsByResource API を使用します。

プロアクティブ評価 (AWS SDKsを有効にする

プロアクティブな評価を有効にする (AWS CLI)

プロアクティブ評価を使用して、デプロイ前のリソースを評価できます。これにより、リージョンのアカウントにあるプロアクティブルールのセットを考慮すると、 AWS リソースを定義するためにリソースプロパティのセットが COMPLIANT か NON_COMPLIANT かを評価することができます。

リソースタイプスキーマは、リソースのプロパティを記述します。リソースタイプスキーマは、AWS CloudFormation レジストリ内のAWS 「パブリック拡張機能」または次の CLI コマンドで確認できます。

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

詳細については、「 AWS CloudFormation ユーザーガイド」の AWS CloudFormation 「レジストリとリソースおよびプロパティタイプのリファレンスによる拡張機能の管理」を参照してください。AWS

> **Note**
>
> プロアクティブルールは、NON_COMPLIANT のフラグが付けられたリソースを修正したり、これらのリソースのデプロイを妨げたりしません。

プロアクティブな評価を有効にするには

put-config-rule コマンドを使用して、EvaluationModes に PROACTIVE を有効にします。

プロアクティブ評価をオンにすると、start-resource-evaluation CLI コマンドと get-resource-evaluation-summary CLI コマンドを使用して、これらのコマンドで指定したリソースが、リージョンのアカウントのプロアクティブルールに照らして NON_COMPLIANT としてフラグが設定されるかどうかを確認できます。

例えば、start-resource-evaluation コマンドを開始します。

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

出力に ResourceEvaluationId が表示されます。

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

次に、ResourceEvaluationId を get-resource-evaluation-summary で使用して評価結果を確認します。

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

次のような出力が表示されます。

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

どのルールがリソースに NON_COMPLIANT のフラグを付けたかなど、評価結果に関する詳細を確認するには、get-compliance-details-by-resource CLI コマンドを使用します。

> **Note**
>
> プロアクティブ評価をサポートするマネージドルールのリストについては、「評価モード別の AWS Config マネージドルールのリスト」を参照してください。

プロアクティブな評価を有効にする (API)

プロアクティブ評価を使用して、デプロイ前のリソースを評価できます。これにより、リージョンのアカウントにあるプロアクティブルールのセットを考慮すると、 AWS リソースを定義するためにリソースプロパティのセットが COMPLIANT か NON_COMPLIANT かを評価することができます。

リソースタイプスキーマは、リソースのプロパティを記述します。リソースタイプスキーマは、AWS CloudFormation レジストリ内のAWS 「パブリック拡張」または次の CLI コマンドで確認できます。

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

詳細については、「 AWS CloudFormation ユーザーガイド」の AWS CloudFormation 「レジストリ、リソース、プロパティタイプのリファレンスによる拡張機能の管理」を参照してください。AWS

> **Note**
> プロアクティブルールは、NON_COMPLIANT のフラグが付けられたリソースを修正したり、これらのリソースのデプロイを妨げたりしません。

ルールのプロアクティブな評価を有効にするには

PutConfigRule アクションを使用して、`EvaluationModes` に `PROACTIVE` を有効にします。

プロアクティブ評価をオンにした後、StartResourceEvaluation API と GetResourceEvaluationSummary API を使用して、これらのコマンドで指定したリソースが、リソースのアカウントのプロアクティブルールに基づいて NON_COMPLIANT としてフラグが設定されるかどうかを確認できます。例えば、StartResourceEvaluation API を開始します。

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

出力に `ResourceEvaluationId` が表示されます。

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

次に、`ResourceEvaluationId` を GetResourceEvaluationSummary API で使用して評価結果を確認します。

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

次のような出力が表示されます。

```
{
```

```
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

どのルールがリソースに NON_COMPLIANT のフラグを付けたかなど、評価結果に関する詳細を確認するには、GetComplianceDetailsByResource API を使用します。

> **Note**
>
> プロアクティブ評価をサポートするマネージドルールのリストについては、「評価モード別の AWS Config マネージドルールのリスト」を参照してください。

ルール評価を Security Hub に送信する

AWS Config ルールを追加したら、ルール評価を送信することもできます AWS Security Hub。 AWS Config と Security Hub の統合により、ルール評価を他の設定ミスやセキュリティ問題とともにトリアージして修正できます。

ルール評価を Security Hub に送信する

Security Hub にルール評価を送信するには、まず AWS Security Hub と をセットアップしてから AWS Config、少なくとも 1 つの AWS Config マネージドルールまたはカスタムルールを追加する必要があります。その後、 AWS Config はすぐに Security Hub へのルール評価の送信を開始します。Security Hub はルール評価を強化して、Security Hub の結果に変換します。

この統合の詳細については、 AWS Security Hub ユーザーガイドの「利用可能な AWS サービス統合」を参照してください。

AWS Config ルールを使用したリソースの評価

カスタムルールを作成するか、マネージドルールを使用すると、 はそれらのルールに照らしてリソース AWS Config を評価します。ルールを適用してリソースのオンデマンド評価を行うことができます。例えば、カスタムルールを作成し、 AWS Config がリソースを正しく評価しているかを確認したり、 AWS Lambda 関数の評価ロジックに問題があるかどうかを判断したりする場合に便利です。

例

1. IAM ユーザーがアクティブなアクセスキーを持っているかどうかを評価するカスタムルールを作成します。
2. AWS Config は、カスタムルールに対してリソースを評価します。
3. アクティブなアクセスキーがない IAM ユーザーがアカウント内に存在します。ルールでは、このリソースに NON_COMPLIANT のフラグが正しく付けられません。
4. ルールを修正して評価をやり直します。
5. ルールを修正したので、リソースが正常に評価され、IAM ユーザーリソースに NON_COMPLIANT のフラグが付けられます。

アカウントにルールを追加するときに、リソースの作成および管理プロセスでリソース AWS Config を評価するタイミングを指定できます。リソースの作成と管理のプロセスは、リソースプロビジョニングと呼ばれます。評価モードを選択して、このプロセスでリソース AWS Config を評価するタイミングを指定します。

ルールに応じて、 はリソースのデプロイ前、リソースのデプロイ後、またはその両方でリソース設定を評価 AWS Config できます。デプロイ前にリソースを評価するのは、プロアクティブ評価です。デプロイ後にリソースを評価するのは、検出評価です。

プロアクティブモード

プロアクティブ評価は、デプロイ前にリソースを評価するために使用します。これにより、 リージョンのアカウントにあるプロアクティブルールのセットを考慮すると、 AWS リソースを定義するためにリソースプロパティのセットが COMPLIANT か NON_COMPLIANT かを評価することができます。

リソースタイプスキーマは、リソースのプロパティを記述します。リソースタイプスキーマは、AWS CloudFormation レジストリ内のAWS 「パブリック拡張」または次の CLI コマンドで確認できます。

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

詳細については、「 AWS CloudFormation ユーザーガイド」の AWS CloudFormation 「レジストリとリソースおよびプロパティタイプのリファレンスによる拡張機能の管理」を参照してください。AWS

> **Note**
> プロアクティブルールは、NON_COMPLIANT のフラグが付けられたリソースを修正したり、これらのリソースのデプロイを妨げたりしません。

リソースの評価

プロアクティブな評価を有効にするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートするリージョンに設定されていることを確認します。サポートされている AWS リージョンのリストについては、Amazon Web Services 全般のリファレンス の「AWS Config のリージョンとエンドポイント」を参照してください。
3. 左のナビゲーションで、ルール を選択します。プロアクティブ評価をサポートするマネージドルールのリストについては、「評価モード別の AWS Config マネージドルールのリスト」を参照してください。
4. ルールを選択し、更新するルールの [Edit rule] (ルールの編集) をクリックします。
5. [Evaluation mode] (評価モード) で、[Turn on proactive evaluation] (プロアクティブな評価をオンにする) を選択し、デプロイ前のリソースの構成設定に対して評価を実行します。
6. [保存] を選択します。

> **Note**
> プロアクティブな評価をオンにするには、`put-config-rule` コマンドを使用して `EvaluationModes` の `PROACTIVE` を有効にするか、PutConfigRule アクションを使用して `EvaluationModes` の `PROACTIVE` を有効にすることもできます。

プロアクティブ評価をオンにした後、StartResourceEvaluation API と GetResourceEvaluationSummary API を使用して、これらのコマンドで指定したリソースが、リソースのアカウントのプロアクティブルールに基づいて NON_COMPLIANT としてフラグが設定されるかどうかを確認できます。

例えば、StartResourceEvaluation API を開始します。

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

出力に `ResourceEvaluationId` が表示されます。

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

次に、`ResourceEvaluationId` を GetResourceEvaluationSummary API で使用して評価結果を確認します。

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

次のような出力が表示されます。

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
```

```
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

どのルールがリソースに NON_COMPLIANT のフラグを付けたかなど、評価結果に関する詳細を確認するには、GetComplianceDetailsByResource API を使用します。

検出モード

検出評価は、デプロイ済みのリソースを評価するために使用します。これにより、既存のリソース構成の設定を評価できます。

リソースの評価 (コンソール)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートするリージョンに設定されていることを確認します。サポートされているリージョンのリストについては、AWS Config の「Amazon Web Services 全般のリファレンスのリージョンとエンドポイント」を参照してください。
3. ナビゲーションペインで ルール を選択します。[Rule] (ルール) ページには、各ルールの名前、関連する修復アクション、およびコンプライアンスステータスが表示されます。
4. テーブルからルールを選択します。
5. [Actions] (アクション) ドロップダウンリストから、[Re-evaluate] (再評価) を選択します。
6. AWS Config は、ルールに対するリソースの評価を開始します。

> **Note**
>
> ルールは 1 分に 1 回再評価できます。別の評価を開始する前に、 AWS Config がルールの評価を完了するのを待つ必要があります。ルールの更新中または削除中に評価を実行することはできません。

リソースの評価 (CLI)

- start-config-rules-evaluationコマンドを使用します。

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

AWS Config は、記録されたリソース設定をルールに対して評価し始めます。リクエストで複数のルールを指定することもできます。

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

リソースの評価 (API)

StartConfigRulesEvaluation アクションを使用します。

AWS Config ルールから評価結果を削除する

がルール AWS Config を評価すると、ルールページまたはルールの詳細ページに評価結果が表示されます。評価結果が正しくない場合や評価をやり直す場合は、ルールの現在の評価結果を削除できます。例えば、ルールでリソースの評価が正しく行われていない場合や最近アカウントからリソースを削除した場合は、評価結果を削除して別の評価を実行できます。

Deleting Evaluation Results (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. AWS Management Console メニューで、リージョンセレクタが AWS Config ルールをサポートする AWS リージョンに設定されていることを確認します。サポートされているリージョンのリストについては、「Amazon Web Services 全般のリファレンス」の「AWS Config のリージョンとエンドポイント」を参照してください。
3. ナビゲーションペインで ルール を選択します。[Rule] (ルール) ページには、各ルールの名前、関連する修復アクション、およびコンプライアンスステータスが表示されます。
4. テーブルからルールを選択します。
5. [Actions] (アクション) ドロップダウンリストから、[Delete results] (結果の削除) を選択します。
6. プロンプトが表示されたら、[Delete] (削除) (大文字と小文字を区別) と入力し、次に [Delete] (削除) を選択します。評価を削除した後は、その評価は取得できません。

7. 評価結果を削除したら、新しい評価を手動で開始できます。

Deleting Evaluation Results (CLI)

- delete-evaluation-results コマンドを使用します。

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

AWS Config は、ルールの評価結果を削除します。

Deleting Evaluation Results (API)

DeleteEvaluationResults アクションを使用します。

AWS Config ルールのトラブルシューティング

AWS Config ルールを削除できない場合や、「An error has occurred with」というエラーが発生した場合のトラブルシューティングについては、次の問題を確認してください AWS Config。

AWS Identity and Access Management (IAM) エンティティには DeleteConfigRule API のアクセス許可があります

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[ユーザー] または [ロール] を選択します。
3. AWS Config ルールの削除に使用したユーザーまたはロールを選択し、アクセス許可ポリシーを展開します。
4. [アクセス許可] タブで、[編集] を選択します。
5. JSON プレビューペインで、IAM ポリシーが DeleteConfigRule API のアクセス許可を許可していることを確認します。

IAM エンティティのアクセス許可の境界が、DeleteConfigRule API を許可します

IAM エンティティにアクセス許可の境界がある場合は、DeleteConfigRule API のアクセス許可が許可されていることを確認してください。

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。

2. ナビゲーションペインで、[ユーザー] または [ロール] を選択します。
3. AWS Config ルールの削除に使用したユーザーまたはロールを選択し、アクセス許可の境界を展開してから、JSON を選択します。
4. JSON プレビューペインで、IAM ポリシーが DeleteConfigRule API のアクセス許可を許可していることを確認します。

> **Warning**
> IAM ユーザーは長期認証情報を保有するため、セキュリティ上のリスクが生じます。このリスクを軽減するために、これらのユーザーにはタスクの実行に必要な権限のみを付与し、不要になったユーザーを削除することをお勧めします。

サービスコントロールポリシー (SCP) が DeleteConfigRule API を許可します

1. 組織の管理アカウントを使用して、https://console.aws.amazon.com/organizations/ で AWS Organizations コンソールを開きます。
2. [アカウント名] で、 AWS アカウントを選択します。
3. [ポリシー] で、[サービスコントロールポリシー] を展開し、アタッチされている SCP ポリシーを書き留めます。
4. ページの上部で、[ポリシー] を選択します。
5. ポリシーを選択した上で、[詳細の表示] をクリックします。
6. JSON プレビューペインで、ポリシーが DeleteConfigRule API を許可していることを確認します。

ルールがサービスにリンクされたルールではありません

セキュリティ標準を有効にすると、 はサービスにリンクされたルール AWS Security Hub を作成します。を使用してこれらのサービスにリンクされたルールを削除することはできません。AWS Config削除ボタンはグレー表示されます。サービスにリンクされたルールを削除するには、「Security Hub ユーザーガイド」の「Disabling a security standard」を参照してください。

進行中の修復アクションはありません

修復アクションが進行中の AWS Config ルールは削除できません。ステップに従って、そのルールに関連付けられている修復アクションを削除します。次に、ルールを再度削除してみてください。

> **Important**
>
> 失敗または成功状態の修復アクションのみを削除します。

のコンフォーマンスパック AWS Config

コンフォーマンスパックは、アカウントとリージョンの単一のエンティティとして、または の組織全体に簡単にデプロイできる AWS Config ルールと修復アクションのコレクションです AWS Organizations。

コンフォーマンスパックは、 AWS Config マネージドルールまたはカスタムルールおよび修復アクションのリストを含む YAML テンプレートを作成することで作成します。 AWS Systems Manager ドキュメント (SSM ドキュメント) を使用してコンフォーマンスパックテンプレートを に保存 AWS し、SSM ドキュメント名を使用してコンフォーマンスパックを直接デプロイすることもできます。テンプレートは、 AWS Config コンソールまたは AWS CLIを使用してデプロイできます。

すぐに開始して AWS 環境を評価するには、サンプルコンフォーマンスパックテンプレートのいずれかを使用します。カスタムコンフォーマンスパックに基づいてコンフォーマンスパックの YAML ファイルをゼロから作成することもできます。

トピック

- のコンフォーマンスパックダッシュボードでのコンプライアンスデータの表示 AWS Config
- のコンフォーマンスパックの前提条件 AWS Config
- リージョンのサポート
- AWS Config のコンフォーマンスパック内のプロセスチェック AWS Config
- のコンフォーマンスパックのサンプルテンプレート AWS Config
- のカスタムコンフォーマンスパック用のテンプレートの作成 AWS Config
- のコンフォーマンスパックのデプロイ AWS Config
- のコンフォーマンスパックの編集 AWS Config
- のコンフォーマンスパックの削除 AWS Config
- のコンフォーマンスパックの詳細とコンプライアンス情報の表示 AWS Config
- のコンフォーマンスパックのコンプライアンス履歴タイムラインの表示 AWS Config
- のコンフォーマンスパックのコンプライアンス履歴のクエリ AWS Config
- 組織内のすべての AWS Config アカウントにおける のコンフォーマンスパックの管理
- のコンフォーマンスパックのトラブルシューティング AWS Config

のコンフォーマンスパックダッシュボードでのコンプライアンスデータの表示 AWS Config

コンフォーマンスパックのメインページには、現在 AWS アカウントにあるコンフォーマンスパックがすべて表示されます。このページには、名前、デプロイステータス、および各コンフォーマンスパックのコンプライアンススコアも表示されます。コンプライアンススコアは、コンフォーマンスパック内の可能なルールとリソースの組み合わせの合計数に対する、コンフォーマンスパック内のコンプライアンスルールとリソースの組み合わせの数の割合です。

このダッシュボードを使用して、コンフォーマンスパックのコンプライアンスレベルを把握し、コンプライアンススコアを使用して修復の進行状況を追跡できます。また、さまざまな要件セット間で比較を実行し、特定の変更またはデプロイがコンフォーマンスパックに与える影響を確認できます。

コンフォーマンスパックのメインページへの移動

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. [Conformance packs] (コンフォーマンスパック) ページに移動します。コンフォーマンスパックとそのコンプライアンススコアを確認します。以下の操作を行うこともできます。
   - 新しいコンフォーマンスパックを追加および設定するには、[Deploy conformance pack] (コンフォーマンスパックをデプロイ) をクリックします。
   - コンフォーマンスパックとそのデータを削除したり、設定を変更したり、配信場所やパラメータなどの追加の詳細を表示したりするには、コンフォーマンスパックを選択してから、[Actions] (アクション) を選択します。

     > **Note**
     >
     > デプロイされたコンフォーマンスパックを編集することはできません。その他の選択内容は、コンフォーマンスパックの名前を選択して [Actions] (アクション) ドロップダウンの [Edit] (編集) を選択すると、いつでも変更できます。

   - コンプライアンス状態の変更履歴を表示するには、コンフォーマンスパックを選択してから、[Conformance pack timeline] (コンフォーマンスパックのタイムライン) を選択します。詳細については、「コンフォーマンスパックのコンプライアンス履歴のタイムラインの表示」を参照してください。

- デプロイステータス、コンプライアンススコア、コンプライアンススコアのタイムライン、およびコンフォーマンスパックのルールを詳細ビューで表示するには、コンフォーマンスパックを選択し、[表示] を選択します。

のコンフォーマンスパックの前提条件 AWS Config

コンフォーマンスパックをデプロイする前に、 AWS Config 記録をオンにします。

トピック

- ステップ 1: AWS Config 録画を開始する (すべてのコンフォーマンスパックで必須)
- ステップ 2: コンフォーマンスパックタイプ別の追加の前提条件

ステップ 1: AWS Config 録画を開始する (すべてのコンフォーマンスパックで必須)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. ナビゲーションペインで [Settings] (設定) を選択します。
3. 記録を開始するには、[Recording is off] (記録はオフ) の [Turn on] (有効) を選択します。プロンプトが表示されたら、[Continue] (続行) をクリックします。

ステップ 2: コンフォーマンスパックタイプ別の追加の前提条件

A. 修復でコンフォーマンスパックを使用するための前提条件

修復を伴うサンプルテンプレートを使用してコンフォーマンスパックをデプロイする前に、修復ターゲットに基づいて、自動化継承ロールやその他のリソースなどの適切な AWS リソースを作成する必要があります。

SSM ドキュメントを使用して修復に使用している既存の自動化ロールがある場合は、そのロールの ARN を直接提供できます。リソースがある場合は、テンプレートにリソースを提供できます。

> **Note**
>
> 組織に修復を伴うコンフォーマンスパックをデプロイする場合、組織の管理アカウント ID を指定する必要があります。それ以外の場合は、組織コンフォーマンスパックのデプロイ時

に、 AWS Config によって、管理アカウント ID をメンバーアカウント ID に自動的に置き換えます。

AWS Config は、自動化実行ロールまたは の AWS CloudFormation 組み込み関数をサポートしていませんConfigRuleName。ロールの正確な ARN を文字列として指定し、組み込み関数なしで完全なルール名を使用する必要があります。

正確な ARN を渡す方法の詳細については、「のコンフォーマンスパックのサンプルテンプレート AWS Config」を参照してください。サンプルテンプレートの使用中に、組織のアカウント ID と管理者アカウント ID を更新します。

B. 1 つ以上のカスタム AWS Config ルールでコンフォーマンスパックを使用するための前提条件

1 つ以上のカスタム AWS Config ルールを含むコンフォーマンスパックをデプロイする前に、 AWS Lambda 関数や対応する実行ロールなどの適切なリソースを作成します。

既存のカスタム AWS Config ルールがある場合は、 AWS Lambda 関数ARNの を直接指定して、そのカスタムルールの別のインスタンスをパックの一部として作成できます。

既存のカスタム AWS Config ルールがない場合は、 AWS Lambda 関数を作成し、Lambda 関数の ARN を使用できます。詳細については、「AWS Config カスタムルール」を参照してください。

AWS Lambda 関数が別の に存在する場合は AWS アカウント、適切なクロスアカウント AWS Lambda 関数認可を使用して AWS Config ルールを作成できます。詳細については、「How to Centrally Manage AWS Config Rules across Multiple AWS アカウント」ブログ記事を参照してください。

Same account bucket policy

がコンフォーマンスパックアーティファクトを保存できるようにする AWS Config には、Amazon S3 バケットを指定し、次のアクセス許可を追加する必要があります。詳細については、バケットの命名規則を参照してください。

JSON

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::delivery-bucket-name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Cross-account bucket policy

がコンフォーマンスパックアーティファクトを保存できるようにする AWS Config には、Amazon S3 バケットを指定し、次のアクセス許可を追加する必要があります。詳細については、バケットの命名規則を参照してください。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
            "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/
[optional] prefix/AWSLogs/AccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": " AWSConfigConformsBucketReadAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
```

```
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/
[optional] prefix/AWSLogs/AccountID/Config/*"
    }
  ]
}
```

> **Note**
>
> クロスアカウントのコンフォーマンスパックをデプロイする場合、Amazon S3 の配信バケットの名前は `awsconfigconforms` で始まる必要があります。

C. Organization Conformance Pack の前提条件

入力テンプレートに自動修復設定がある場合は、その修復のオートメーション実行ロール ARN をテンプレートで指定します。指定した名前のロールが、組織のすべてのアカウント (管理およびメンバー) に存在することを確認します。`PutOrganizationConformancePack` を呼び出す前に、すべてのアカウントでこのロールを作成する必要があります。このロールは、手動で作成することも、AWS CloudFormation スタックセットを使用してすべてのアカウントで作成することもできます。

テンプレートが AWS CloudFormation 組み込み関数を使用して特定の変数`Fn::ImportValue`をインポートする場合、その変数は組織内のすべてのメンバーアカウント`Export Value`で として定義する必要があります。

カスタム AWS Config ルールについては、「How to Centrally Manage AWS Config Rules across Multipleblog AWS アカウント to setup proper permissions」を参照してください。

組織のバケットポリシー:

がコンフォーマンスパックアーティファクトを保存できるようにする AWS Config には、Amazon S3 バケットを指定し、次のアクセス許可を追加する必要があります。詳細については、バケットの命名規則を参照してください。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/
config-conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/
config-conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

> **Note**
> コンフォーマンスパックを組織にデプロイする場合、Amazon S3 の配信バケットの名前は `awsconfigconforms` で始まる必要があります。

リージョンのサポート

コンフォーマンスパックは、次のリージョンでサポートされています。

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
米国西部 (北カリフォルニア)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル	
アジアパシフィック (ハイデラバード)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Organization のメンバーアカウント間でコンフォーマンスパックをデプロイすることは AWS 、次のリージョンでサポートされています。

リージョン名	リージョン	エンドポイント	プロトコル	
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
米国西部 (北カリフォルニア)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
アジアパシフィック (ハイデラバード)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config のコンフォーマンスパック内のプロセスチェック AWS Config

プロセスチェックは、コンフォーマンスパックの一部として検証が必要な外部タスクと内部タスクを追跡できる AWS Config ルールの一種です。これらのチェックは、既存のコンフォーマンスパックまたは新しいコンフォーマンスパックに追加できます。urations や手動チェックを含むすべてのコンプライアンスを 1 AWS Configか所で追跡できます。

プロセスチェックを使用すると、要件とアクションのコンプライアンスを 1 か所で一覧表示できます。これらのプロセスチェックは、コンプライアンス制度に基づくコンフォーマンスパックの適用範囲を拡大するのに役立ちます。手動による検証と追跡が必要なプロセスとアクションを追跡する新しいプロセスチェックを追加することで、コンフォーマンスパックをさらに拡張できます。これによ

り、コンフォーマンスパックは、コンプライアンス体制の urations AWS Configと手動プロセスに関する詳細を提供するテンプレートになります。

コンフォーマンスパック内のリソース設定の変更に関連付けられていないプロセスのコンプライアンスを、プロセスチェックとして追跡し管理できます。例えば、オフサイトの場所にメディアバックアップを保存するために、PCI-DSS コンプライアンス要件を追跡するプロセスチェックを追加できます。PCI-DSS のガイドラインまたは組織のガイダンスに従って、このコンプライアンスを手動で評価します。

リージョンの可用性: コンフォーマンスパックを使用したプロセスチェックは、コン AWS Config フォーマンスパックが利用可能なすべての AWS リージョン で利用できます。詳細については、「リージョンのサポート」を参照してください。

トピック

- プロセスチェックを作成するためのサンプルコンフォーマンスパックのテンプレート
- コンフォーマンスパック内にプロセスチェックを含める
- プロセスチェックのコンプライアンスステータスの変更
- プロセスチェックの表示と編集 (コンソール)

プロセスチェックを作成するためのサンプルコンフォーマンスパックのテンプレート

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

2 つのテンプレート (CIS AWS Foundations Benchmark v1.4 Level 1 に関する運用上のベストプラクティス テンプレートと CIS AWS Foundations Benchmark v1.4 Level 2 の運用上のベストプラクティス テンプレート) を参照してください。

コンフォーマンスパック内にプロセスチェックを含める

1. コンフォーマンスパックテンプレートにプロセスチェックを追加します。「プロセスチェックを作成するためのサンプルコンフォーマンスパックのテンプレート」を参照してください。

```
Resources:
  ConfigEnabledAllRegions:
    Properties:
      ConfigRuleName: Config-Enabled-All-Regions
      Description: Ensure AWS Config is enabled in all Regions.
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

2. プロセスチェックの名前を入力します。
3. プロセスチェックの説明を入力します。
4. 適合パックをデプロイします。詳細については、「のコンフォーマンスパックのデプロイ AWS Config」を参照してください。

プロセスチェックのコンプライアンスステータスの変更

プロセスチェックのコンプライアンスステータスは、 AWS Config コンソール、、 AWS CLIおよび APIs を使用して変更できます。

Change Compliance Status for Process Checks (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. AWS Config ルールページに移動します。
3. テンプレートで指定したプロセスチェックの名前と、コンフォーマンスパックの識別子を選択します。

> **Note**
> 同じコンフォーマンスパックからのプロセスチェックには、すべて同じプレフィックスが付いています。

4. Rule details (ルールの詳細) ページでは、ルールを編集することはできませんが、ルールのコンプライアンスを編集することができます。[Manual compliance] (手動コンプライアンス) セクションで、[Edit compliance] (コンプライアンスの編集) をクリックします。
5. ドロップダウンリストから適切なコンプライアンスを選択します。
6. (オプション) コンプライアンスステータスの説明を入力します。
7. [保存] を選択します。

Change the Compliance Status for Process Checks (AWS CLI)

AWS Command Line Interface () を使用して、コンフォーマンスパック内のプロセスチェックのコンプライアンスを更新できますAWS CLI。

をローカルマシン AWS CLI にインストールするには、 AWS CLI ユーザーガイドの「 AWS CLIのインストール」を参照してください。

必要に応じて、「」と入力`AWS Config ure`して、コンフォーマンスパックが利用可能な リージョンを使用する AWS CLI AWS ように AWS Config を設定します。

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. プロセスチェックのコンプライアンスを更新するには、次のコマンドを入力します。`ComplianceResourceId` には `Account ID` を入力し、ルールの名前を含めます。

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. Enter キーを押してコマンドを実行します。

Change the Compliance Status for Process Checks (API)

デプロイが完了したら、`PutExternalEvaluation` API を使用してプロセスチェックの評価とコンプライアンスを更新します。詳細については、PutExternalEvaluation を参照してください。

プロセスチェックの表示と編集 (コンソール)

プロセスチェックは、コンプライアンス状態がプロセスチェックに追加された後にのみ表示できます。特定のコンフォーマンスパックを選択して、そのコンフォーマンスパック内のすべてのプロセスチェックを表示します。ここには、準拠ステータスおよび非準拠ステータスのプロセスチェックのリストが表示されます。

これはサービスがリンクされているルールであるため、[Rule details] (ルールの詳細) ページでプロセスチェックを編集することはできません。

> **Note**
>
> ただし、[コンプライアンスの編集] をクリックし、[準拠]、[非準拠]、または [該当なし] から適切な値を選択すると、プロセスチェックのコンプライアンスを更新することができます。

プロセスチェックを追加したコンフォーマンスパックから、プロセスチェックを編集または削除できます。

のコンフォーマンスパックのサンプルテンプレート AWS Config

AWS Config コンソールに表示されるコンフォーマンスパック YAML テンプレートを次に示します。各コンフォーマンスパックテンプレート内で、1 つ以上の AWS Config ルールと修復アクションを使用できます。コンフォーマンスパックにリストされている AWS Config ルールは、 AWS Config マネージドルールや AWS Config カスタムルールにすることができます。すべてのコンフォーマンスパックテンプレートは、GitHub からダウンロードできます。

> **Important**
>
> コンフォーマンスパックは、マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成するのに役立つ汎用コンプライアンスフレームワークを提供します。 AWS コンフォーマンスパックのサンプルテンプレートは、環境に適した異なるルールまたは追加のルール、入力パラメータ、および修復アクションを含む独自のコンフォーマンスパックを作成するのに役立ちます。コンプライアンス標準や業界ベンチマークに関連するテンプレートなど、サンプルテンプレートは、特定のガバナンス標準へのコンプライアンスを保証するようには設計されていません。また、社内の取り組みに取って代わることも、コンプライアンス評価に合格することを保証することもできません。

> **Note**
>
> コンフォーマンスパックをデプロイするリージョンで利用可能なルール (リージョンの可用性別の AWS Config マネージドルールのリスト) を確認し、デプロイする前にそのリージョンでまだ利用できないルールのテンプレートを修正することをお勧めします。

トピック

- AWS Control Tower Detective ガードレールコンフォーマンスパック
- ABS CCIG 2.0 マテリアルワークロードに関する運用上のベストプラクティス
- ABS CCIG 2.0 標準ワークロードに関する運用上のベストプラクティス
- ACSC の Essential 8 に関する運用上のベストプラクティス
- ACSC の「ISM」に関する運用上のベストプラクティス
- AI と機械学習に関する運用面のベストプラクティス
- Amazon API Gateway 運用のベストプラクティス
- Amazon CloudWatch に関する運用上のベストプラクティス
- Amazon DynamoDB に関する運用上のベストプラクティス
- Amazon S3 に関する運用上のベストプラクティス
- APRA の「CPG 234」に関する運用上のベストプラクティス
- アセット管理に関する運用上のベストプラクティス
- の運用のベストプラクティス AWS Backup
- AWS Identity and Access Management に関する運用上のベストプラクティス
- AWS Well-Architected フレームワークの信頼性の柱に関する運用上のベストプラクティス
- AWS Well-Architected フレームワークのセキュリティの柱に関する運用上のベストプラクティス
- BCP と DR に関する運用上のベストプラクティス
- BNM の「RMiT」に関する運用上のベストプラクティス
- カナダサイバーセキュリティセンター (CCCS) 中規模クラウド制御プロファイルに関する運用面のベストプラクティス
- CIS AWS Foundations Benchmark v1.4 Level 1 に関する運用上のベストプラクティス
- CIS AWS Foundations Benchmark v1.4 Level 2 の運用上のベストプラクティス
- CIS の「Critical Security Controls v8 IG1」に関する運用上のベストプラクティス

- CIS の「Critical Security Controls v8 IG2」に関する運用上のベストプラクティス
- CIS の「Critical Security Controls v8 IG3」に関する運用上のベストプラクティス
- CIS の「Top 20」に関する運用上のベストプラクティス
- CISA サイバーエッセンシャル 運用のベストプラクティス
- Criminal Justice Information Services (CJIS) の運用のベストプラクティス
- CMMC 2.0 Level 1 に関する運用上のベストプラクティス
- CMMC 2.0 Level 2 に関する運用上のベストプラクティス
- コンピューティングサービスに関する運用上のベストプラクティス
- データの回復性に関する運用上のベストプラクティス
- データベースサービスに関する運用上のベストプラクティス
- データレイクと分析サービスに関する運用上のベストプラクティス
- DevOP s 運用のベストプラクティス
- EC2 に関する運用上のベストプラクティス
- 暗号化とキー管理に関する運用上のベストプラクティス
- SME 向け ENISA サイバーセキュリティガイドの運用上のベストプラクティス
- 「Esquema Nacional de Seguridad (ENS) Low」に関する運用のベストプラクティス
- 「Esquema Nacional de Seguridad (ENS) Medium」に関する運用のベストプラクティス
- 「Esquema Nacional de Seguridad (ENS) High」に関する運用のベストプラクティス
- FDA Title 21 CFR Part 11 の運用のベストプラクティス
- FedRAMP (Low) の運用のベストプラクティス
- FedRAMP(Moderate) に関する運用上のベストプラクティス
- FedRAMP (High Part 1) の運用のベストプラクティス
- FedRAMP (High Part 2) の運用のベストプラクティス
- FFIEC に関する運用上のベストプラクティス
- ドイツのクラウドコンピューティングコンプライアンス条件カタログ (C5) の運用上のベストプラクティス
- グラムリーチブライリー法 (GLBA) に関する運用上のベストプラクティス
- GxP EU Annex 11 に関する運用上のベストプラクティス
- HIPAA Security の運用のベストプラクティス
- IRS 1075 に関する運用上のベストプラクティス

- K-ISMS の運用のベストプラクティス
- ロードバランシングの運用のベストプラクティス
- ログ記録に関する運用上のベストプラクティス
- サービスの管理およびガバナンスの運用のベストプラクティス
- シンガポール金融管理局の「Notice 655」の運用のベストプラクティス
- MAS TRMGの運用のベストプラクティス
- モニタリングの運用のベストプラクティス
- NBC の「TRMG」の運用のベストプラクティス
- NERC CIP BCSI に関する運用上のベストプラクティス
- NCSC Cloud Security Principles に関する運用上のベストプラクティス
- NCSC の「Cyber Assesment Framework」に関する運用上のベストプラクティス
- ネットワークおよびコンテンツ配信サービスの運用のベストプラクティス
- NIST の「800-53 rev 4」の運用のベストプラクティス
- NIST の「800-53 rev 5」の運用のベストプラクティス
- NIST 800 171 に関する運用上のベストプラクティス
- NIST の「800 172」の運用のベストプラクティス
- NIST の「800 181」の運用のベストプラクティス
- NIST の「1800 25」に関する運用上のベストプラクティス
- NIST の「CSF」に関する運用上のベストプラクティス
- NIST プライバシーフレームワーク v1.0 オペレーションのベストプラクティス
- NYDFS 23 の運用のベストプラクティス
- NZISM 3.8 の運用上のベストプラクティス
- PCI DSS 3.2.1 運用のベストプラクティス
- PCI DSS 4.0 の運用上のベストプラクティス (グローバルリソースタイプを除く)
- PCI DSS 4.0 の運用上のベストプラクティス (グローバルリソースタイプを含む)
- パブリックにアクセス可能なリソースの運用のベストプラクティス
- RBI の「Cyber Security Framework for UCBs」に関する運用上のベストプラクティス
- RBI の「MD-ITF」の運用のベストプラクティス
- セキュリティ、ID、コンプライアンスの運用のベストプラクティス
- サーバーレスの運用のベストプラクティス

- ストレージサービスの運用のベストプラクティス
- SWIFT CSP の運用のベストプラクティス
- Amazon Elastic Container Service (Amazon ECS) のセキュリティのベストプラクティス
- Amazon Elastic File System (Amazon EFS) のセキュリティのベストプラクティス
- Amazon Elastic Kubernetes Service (Amazon EKS) でのセキュリティに関するベストプラクティス
- Amazon CloudFront のセキュリティのベストプラクティス
- Amazon OpenSearch Service のセキュリティベストプラクティス
- Amazon Redshift のセキュリティベストプラクティス
- Amazon Relational Database Service (Amazon RDS) でのセキュリティに関するベストプラクティス
- AWS Auto Scalingのセキュリティのベストプラクティス
- AWS CloudTrailのセキュリティのベストプラクティス
- AWS CodeBuildのセキュリティのベストプラクティス
- Amazon ECR のセキュリティのベストプラクティス
- AWS Lambdaのセキュリティのベストプラクティス
- AWS Network Firewallのセキュリティのベストプラクティス
- Amazon SageMaker AI のセキュリティのベストプラクティス
- AWS Secrets Managerのセキュリティのベストプラクティス
- AWS WAFのセキュリティのベストプラクティス
- 修正アクションを含むテンプレートの例

AWS Control Tower Detective ガードレールコンフォーマンスパック

このコンフォーマンスパックには、 AWS Control Tower Detective ガードレールに基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは GitHub の「AWS Control Tower Detective Guardrails Conformance Pack」で入手できます。

ABS CCIG 2.0 マテリアルワークロードに関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、ABS Cloud Computing 実装ガイド 2.0 - マテリアルワークロードと AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の ABS Cloud Computing 実装ガイドのコントロールに関連付けられます。ABS Cloud Computing 実装ガイドによるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-2-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
section4a-govern-the-cloud-2-material-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティア

コントロール ID	AWS 設定ルール	ガイダンス
		ラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-3-material-workloads	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4a-govern-the-cloud-3-material-workloads	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
section4a-govern-the-cloud-3-standard-workloads	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。6.4.7

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。6.4.7

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-material-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
section4b-design-and-secure-the-cloud-3-material-workloads	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-material-workloads	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
section4b-design-and-secure-the-cloud-3-material-workloads	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-material-workloads	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-material-workloads	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-material-workloads	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
section4b-design-and-secure-the-cloud-4-material-workloads	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
section4b-design-and-secure-the-cloud-4-material-workloads	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-4-material-workloads	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
section4b-design-and-secure-the-cloud-4-material-workloads	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
section4b-design-and-secure-the-cloud-4-material-workloads	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-4-material-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
section4b-design-and-secure-the-cloud-4-material-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-material-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
section4b-design-and-secure-the-cloud-5-material-workloads	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。
section4b-design-and-secure-the-cloud-5-material-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。 root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-5-material-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-5-material-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-5-material-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
section4b-design-and-secure-the-cloud-6-material-workloads	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-material-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-material-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-material-workloads	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-material-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-8-material-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-material-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-9-material-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
section4b-design-and-secure-the-cloud-9-material-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-material-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-9-material-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
section4b-design-and-secure-the-cloud-10-material-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-10-material-workloads	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-10-material-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
section4b-design-and-secure-the-cloud-10-material-workloads	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
section4b-design-and-secure-the-cloud-10-material-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-10-material-workloads	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
section4b-design-and-secure-the-cloud-10-material-workloads	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-10-material-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
section4b-design-and-secure-the-cloud-10-material-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-material-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
section4b-design-and-secure-the-cloud-11-material-workloads	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
section4b-design-and-secure-the-cloud-11-material-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-11-material-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
section4b-design-and-secure-the-cloud-11-material-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
section4b-design-and-secure-the-cloud-11-material-workloads	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-11-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
section4b-design-and-secure-the-cloud-11-material-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-11-material-workloads	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
section4b-design-and-secure-the-cloud-11-material-workloads	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-11-material-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-11-material-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
section4b-design-and-secure-the-cloud-11-material-workloads	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-11-material-workloads	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロンググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-material-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。
section4b-design-and-secure-the-cloud-14-material-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-material-workloads	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
section4b-design-and-secure-the-cloud-14-material-workloads	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-material-workloads	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
section4b-design-and-secure-the-cloud-14-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-material-workloads	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
section4b-design-and-secure-the-cloud-14-material-workloads	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-material-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-material-workloads	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
section4b-design-and-secure-the-cloud-15-material-workloads	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-material-workloads	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
section4b-design-and-secure-the-cloud-15-material-workloads	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
section4c-run-the-cloud-2-material-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-2-material-workloads	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained (process check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。
section4c-run-the-cloud-4-material-workloads	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
section4c-run-the-cloud-4-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-4-material-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-6-material-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
section4c-run-the-cloud-6-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-6-material-workloads	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for ABS CCIG 2.0 Material Workloads」で入手できます。

ABS CCIG 2.0 標準ワークロードに関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、ABS Cloud Computing 実装ガイド 2.0 - 標準ワークロードと AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の ABS Cloud Computing Implementation Guide コントロールに関連付けられます。ABS Cloud Computing 実装ガイドによるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした

コントロール ID	AWS 設定ルール	ガイダンス
		AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
section4a-govern-the-cloud-3-standard-workloads	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。6.4.7

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。6.4.7

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
section4b-design-and-secure-the-cloud-12-standard-workloads	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
section4c-run-the-cloud-3-standard-workloads	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
section4c-run-the-cloud-3-standard-workloads	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained (process check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	AWS 設定ルール	ガイダンス
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for ABS CCIG 2.0 Standard Workloads」で入手できます。

ACSC の Essential 8 に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、オーストラリアサイバーセキュリティセンター (ACSC) の Essential Eight Maturity Model と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の ACSC Essential Eight コントロールに関連付けられます。ACSC の Essential Eight によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。Config ルールへのマッピングの一部は、より規範的なセクションではなく、より高以下のセクション (例えば、サイバーセキュリティインシデントの範囲を制限するための緩和戦略) 向けとなっています。

コンフォーマンスパックのサンプルテンプレートには、オーストラリア連邦によって作成された「ACSC | Essential Eight」 に記載の ACSC Essential 8 によるコントロールへのマッピングが含まれています。クリエイティブコモンズの Attribution 4.0 International Public License に基づくフレームワークのライセンスと、フレームワークの著作権情報 (保証の免責を含む) については、「ACSC | Copyright」でご確認ください。

コントロール ID	AWS 設定ルール	ガイダンス
Application_control	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これら

コントロール ID	AWS 設定ルール	ガイダンス
		のウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
Application_control	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Application_control	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
Application_control	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。
Application_control	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Application_control	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。
Application_control	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Patch_applications	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
Patch_applications	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
Patch_applications	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 は AWS プラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。
Patch_applications	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	AWS 設定ルール	ガイダンス
Patch_applications	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
Patch_applications	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Patch_applications	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
Restrict_administrative_privileges	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
Restrict_administrative_privileges	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
Restrict_administrative_privileges	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Restrict_administrative_privileges	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。
Restrict_administrative_privileges	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。
Restrict_administrative_privileges	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Restrict_administrative_privileges	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。
Restrict_administrative_privileges	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。
Restrict_administrative_privileges	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Restrict_administrative_privileges	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Restrict_administrative_privileges	rds-instance-iam-authentication-enabled	システムおよびアセットへのアクセスを制御するために、Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。これにより、データベースに出入りするネットワークトラフィックが、Secure Sockets Layer (SSL) を使用して暗号化されるようになります。認証は外部で管理されるため、ユーザー認証情報をデータベースに保存する必要はありません。
Restrict_administrative_privileges	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	AWS 設定ルール	ガイダンス
Restrict_administrative_privileges	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
Restrict_administrative_privileges	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Restrict_administrative_privileges	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
Restrict_administrative_privileges	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Patch_operating_systems	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
多要素認証	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
多要素認証	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
多要素認証	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
多要素認証	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
多要素認証	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
通常のバックアップ	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
通常のバックアップ	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
通常のバックアップ	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
通常のバックアップ	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
通常のバックアップ	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
通常のバックアップ	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
通常のバックアップ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
通常のバックアップ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	AWS 設定ルール	ガイダンス
通常のバックアップ	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
通常のバックアップ	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要件を反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
通常のバックアップ	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
通常のバックアップ	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
通常のバックアップ	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for ACSC Essential 8」で入手できます。

ACSC の「ISM」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、オーストラリアサイバーセキュリティセンター (ACSC) 情報セキュリティマニュアル (ISM) 2020-06 と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の ISM コントロールに関連付けられます。「ISM」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コンフォーマンスパックのサンプルテンプレートには、オーストラリア連邦によって作成された「Australian Government Information Security Manual」 に記載の「ISM」フレームワークによるコントロールへのマッピングが含まれています。クリエイティブコモンズの Attribution 4.0 International Public License に基づくフレームワークのライセンスと、フレームワークの著作権情報 (保証の免責を含む) については、「ACSC | Copyright」でご確認ください。

コントロール ID	AWS 設定ルール	ガイダンス
43	response-plan-exists-maintained (process check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。
252	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
261	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
261	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られま

コントロール ID	AWS 設定ルール	ガイダンス
		す。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
261	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
298	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	AWS 設定ルール	ガイダンス
298	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
298	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	AWS 設定ルール	ガイダンス
298	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
380	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。
459	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
459	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
459	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
459	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
459	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
459	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
459	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
459	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
459	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
459	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
459	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
459	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
459	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
459	codebuild-project-artifact-encryption	保管中の機密データを保護するために、 AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。
459	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
459	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
459	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
459	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
459	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
459	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
580	audit-log-policy-exists (Process check)	組織の口グ要件を定義する、監査口グの管理ポリシーを確立して維持します。これには監査口グのレビューと保持が含まれますが、これらに限定されるわけではありません。

コントロール ID	AWS 設定ルール	ガイダンス
634	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
859	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	AWS 設定ルール	ガイダンス
974	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
974	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
1139	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号 という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1173	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
1173	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1173	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
1173	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
1173	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
1228	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1240	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
1240	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
1271	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
1271	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	AWS 設定ルール	ガイダンス
1277	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
1277	rds-instance-iam-authentication-enabled	システムとアセットへのアクセスを制御するために、Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。これにより、データベースに出入りするネットワークトラフィックが、Secure Sockets Layer (SSL) を使用して暗号化されるようになります。認証は外部で管理されるため、ユーザー認証情報をデータベースに保存する必要はありません。
1277	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
1380	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
1380	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
1380	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 は AWS プラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。
1380	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	AWS 設定ルール	ガイダンス
1380	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
1380	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
1380	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
1380	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
1380	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
1380	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
1380	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。
1380	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。
1380	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1380	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。
1380	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。
1380	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
1380	rds-instance-iam-authentication-enabled	システムとアセットへのアクセスを制御するために、Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。これにより、データベースに出入りするネットワークトラフィックが、Secure Sockets Layer (SSL) を使用して暗号化されるようになります。認証は外部で管理されるため、ユーザー認証情報をデータベースに保存する必要はありません。
1380	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	AWS 設定ルール	ガイダンス
1380	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
1380	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1380	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
1380	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
1388	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	AWS 設定ルール	ガイダンス
1388	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
1401	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
1401	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
1401	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
1401	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
1401	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1402	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1404	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。
1405	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1405	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
1405	multi-region-cloudtrail-enabled	MULTI_REGION_CLOUD_TRAIL_ENABLED
1405	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1405	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
1405	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
1405	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1405	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
1405	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1405	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
1405	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
1405	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
1405	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1405	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
1405	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。
1405	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、Open Search へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。

コントロール ID	AWS 設定ルール	ガイダンス
1405	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
1490	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
1490	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
1490	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。
1490	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
1490	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。
1490	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
1501	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	AWS 設定ルール	ガイダンス
1504	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
1504	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
1504	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
1504	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1504	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
1509	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1509	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
1509	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
1509	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
1509	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
1509	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS 設定ルール	ガイダンス
1509	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
1509	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
1509	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1509	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
1509	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
1509	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
1509	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1509	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
1509	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。
1509	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、Open Search へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。

コントロール ID	AWS 設定ルール	ガイダンス
1509	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
1511	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
1511	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
1511	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
1511	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
1511	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1511	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
1511	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1511	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
1511	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	AWS 設定ルール	ガイダンス
1511	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1511	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要件を反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1511	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定:35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1511	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
1511	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1511	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
1511	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要件を反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1511	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
1515	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
1515	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
1515	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1515	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
1515	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	AWS 設定ルール	ガイダンス
1515	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
1515	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
1515	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
1515	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1515	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要件を反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1515	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
1515	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1515	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。
1536	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1537	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
1537	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1552	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
1552	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
1552	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
1552	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
1552	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
1579	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
1580	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
1580	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
1580	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
1650	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1650	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
1650	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
1650	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1650	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
1650	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
1650	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1650	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
1650	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1650	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
1650	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
1650	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
1650	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1650	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
1650	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。
1650	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、Open Search へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。

コントロール ID	AWS 設定ルール	ガイダンス
1650	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
1657	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
1657	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
1657	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
1657	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。
1657	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。
1657	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。

コントロール ID	AWS 設定ルール	ガイダンス
1657	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
1661	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1661	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
1661	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
1661	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1661	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
1661	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
1661	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1661	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
1661	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1661	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
1661	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
1661	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
1661	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1661	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
1679	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
1679	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
1679	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
1679	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
1679	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1680	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
1680	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
1680	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
1680	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1680	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
1681	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
1681	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
1681	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
1681	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
1681	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
1683	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
1683	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1690	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
1690	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
1690	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 は AWS プラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。
1690	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	AWS 設定ルール	ガイダンス
1690	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
1690	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
1690	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1691	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
1691	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
1691	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 は AWS プラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。
1691	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	AWS 設定ルール	ガイダンス
1691	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
1691	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
1691	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1693	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
1693	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
1693	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 は AWS プラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。
1693	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	AWS 設定ルール	ガイダンス
1693	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
1693	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
1693	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
1694	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	AWS 設定ルール	ガイダンス
1695	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
1707	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
P1	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
P1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
P3	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	AWS 設定ルール	ガイダンス
P5	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
P7	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
P7	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
P7	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
P7	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
P8	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
P9	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
P9	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要件を反映する必要があります。
P9	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
P9	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
P9	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定:35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
P9	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
P9	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
P9	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
P9	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
P9	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
P9	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	AWS 設定ルール	ガイダンス
P9	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
P9	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
P9	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。
P10	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
P10	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
P10	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
P10	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
P10	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
P11	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for ACSC ISM」で入手できます。

AI と機械学習に関する運用面のベストプラクティス

このコンフォーマンスパックには、AI と ML に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for AI and ML」で入手できます。

Amazon API Gateway 運用のベストプラクティス

このコンフォーマンスパックには、Amazon API Gateway の使用に基づく AWS Config ルールが含まれています AWS。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Amazon API Gateway」で入手できます。

Amazon CloudWatch に関する運用上のベストプラクティス

このコンフォーマンスパックには、Amazon CloudWatch の使用に基づく AWS Config ルールが含まれています AWS。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Amazon CloudWatch に関する運用上のベストプラクティス」で入手できます。

Amazon DynamoDB に関する運用上のベストプラクティス

テンプレートは、GitHub の「Operational Best Practices for Amazon DynamoDB」で入手できます。

Amazon S3 に関する運用上のベストプラクティス

テンプレートは、GitHub の「Operational Best Practices for Amazon S3」で入手できます。

APRA の「CPG 234」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、オーストラリア連邦規則局 (APRA) CPG 234 と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の APRA CPG 234 コントロールに関連付けられます。APRA の「CPG 234」によるコントロールを、複数の Config ルールに関連付けることができます これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックのサンプルテンプレートには、オーストラリア連邦によって作成された Prudential Practice Guide: CPG 234 Information Security に記載されている「APRA CPG 234 2019」によるコントロールへのマッピングが含まれています。Creative Commons Australia

Attribution 3.0 Licence に基づくフレームワークのライセンスとフレームワークの著作権に関する情報 (保証の免責事項を含む) については、「APRA | Copyright」を参照してください。

コントロール ID	AWS 設定ルール	ガイダンス
36a	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
36a	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
36a	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
36b	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
36b	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
36b	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	AWS 設定ルール	ガイダンス
36b	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
36b	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36b	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。
36b	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	AWS 設定ルール	ガイダンス
36c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
36c	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
36c	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
36c	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36c	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
36c	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
36c	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
36c	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
36c	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
悪意のあるコードを検出すると、[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]とともに、アラートが[Assignment: organization-defined personnel or roles]に送信されます。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
36e	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager シークレットのローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
36e	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
36e	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
36e	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
36e	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
36e	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
36e	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
36e	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
36e	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
36e	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
36e	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
36e	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
36e	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
36e	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
36e	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36e	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
36e	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
36e	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	AWS 設定ルール	ガイダンス
36e	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
36e	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
36e	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
36e	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36e	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。
36e	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
36e	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
36e	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
36e	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
36f	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
36f	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
36f	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
36f	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
36f	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
36f	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
36f	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
36f	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
36f	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
36f	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
36f	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
36f	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
36f	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36f	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
36f	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
36f	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
36f	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36f	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
36f	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
36f	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
36f	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
36f	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
36f	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	AWS 設定ルール	ガイダンス
36f	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
36f	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	AWS 設定ルール	ガイダンス
36f	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
36f	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
36f	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
36f	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
36g	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
36g	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
36g	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
36h	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
36h	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
36h	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
36h	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
36h	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
36h	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
36h	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36h	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。
36i	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	AWS 設定ルール	ガイダンス
36i	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36i	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36i	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
36i	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。
36i	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	AWS 設定ルール	ガイダンス
36i	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。
36i	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
36i	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
36i	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
36i	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
36j	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
36j	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
36j	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
36j	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
36j	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	AWS 設定ルール	ガイダンス
36j	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
36j	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
36j	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	AWS 設定ルール	ガイダンス
36j	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。
36j	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
36j	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
36l	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
36l	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
36l	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
36l	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
36l	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
36l	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
36l	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
36l	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
36l	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
36l	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
36l	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
36l	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
36l	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
36l	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
36l	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
36l	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。
36l	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
39(a)(b)(d)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
39(a)(b)(d)	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
39(a)(b)(d)	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
40	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	AWS 設定ルール	ガイダンス
40	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
40	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	AWS 設定ルール	ガイダンス
40	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
44a	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
44a	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
44a	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
44b	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
44b	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	AWS 設定ルール	ガイダンス
44b	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
44c	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
44c	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
44c	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
44c	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
45	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
45	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
45	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
45	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
45	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
45	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
45	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
45	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
45	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
45	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
45	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
45	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
45	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
45	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
45	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
45	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
45	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
45	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
45	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
45	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
45	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
45	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
45	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
45	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
45	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。
45	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
45	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
45	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
45	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
45	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
45	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
45	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
45	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。 (AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
45	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	AWS 設定ルール	ガイダンス
45	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
45	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
45	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
45	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
45	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
45	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。
45	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
45	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
45	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
47c	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
47c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
47c	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
47c	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
47c	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
47c	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
47c	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
52c	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
52c	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
52c	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
52c	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
52c	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
52c	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
52c	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
52c	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
52c	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
52c	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
52c	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
52c	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
52c	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
52c	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	AWS 設定ルール	ガイダンス
52c	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
52c	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
52c	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
52c	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
52d	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
52d	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
52d	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
52d	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
52d	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
52d	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
52d	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
52d	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
52d	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
52d	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
52d	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
52d	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
52d	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
52d	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
52d	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
52d	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
52d	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
52d	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
52d	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。
52d	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
52d	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
52d	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
52d	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
52e	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
52e	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
53	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
53	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
53	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
53	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
53	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
53	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
53	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
53	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
53	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
53	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
53	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
53	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
53	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
53	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
53	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
53	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
53	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
53	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
53	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	AWS 設定ルール	ガイダンス
53	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
53	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	AWS 設定ルール	ガイダンス
53	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
53	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
54	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
54	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
54	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
54	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
54	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
54	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
54	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
54	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
54	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
54	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
54	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
54	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
54	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
54	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
54	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
54	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
54	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
54	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
54	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
54	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
54	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
54	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
54	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
54	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
54	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
54	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
55	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
55	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
67	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
67	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
67	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
67	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
67	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
67	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
67	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
67	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
67	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
67	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	AWS 設定ルール	ガイダンス
67	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。
67	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
67	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
67	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
67	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
67	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
67	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
67	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
68	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
68	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
73	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
73	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(b)(h)	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(b)(h)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AttachmentA_1(b)(h)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(b)(h)	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AttachmentA_1(b)(h)	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(b)(h)	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(b)(h)	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(b)(h)	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
AttachmentA_1(b)(h)	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(b)(h)	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
AttachmentA_1(c)	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(c)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AttachmentA_1(e)	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(e)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AttachmentA_1(e)	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(e)	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
AttachmentA_1(e)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AttachmentA_1(e)	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(e)	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
AttachmentA_1(e)	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(e)	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(e)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
AttachmentA_1(e)	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(e)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
AttachmentA_1(e)	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentA_1(e)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
AttachmentA_1(e)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
AttachmentB_1	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AttachmentC_4	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AttachmentC_4	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
AttachmentC_4	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
AttachmentC_4	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
AttachmentC_4	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
AttachmentC_4	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。 (AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
AttachmentC_4	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_4	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AttachmentC_5	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_5	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
AttachmentC_5	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_5	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_5	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基本的なセキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_6	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
AttachmentC_6	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_6	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
AttachmentC_7(c)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(h)	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
AttachmentC_7(h)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AttachmentC_7(h)	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(h)	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
AttachmentC_7(h)	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(h)	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
AttachmentC_7(h)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(h)	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(h)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(h)	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
AttachmentC_7(h)	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(h)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
AttachmentC_7(h)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(h)	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AttachmentC_7(h)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(i)	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。
AttachmentC_7(j)	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(j)	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
AttachmentC_7(j)	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_7(j)	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
AttachmentC_8	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
AttachmentC_8	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_8	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AttachmentC_8	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
AttachmentC_8	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_8	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_8	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_8	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
AttachmentC_8	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_8	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
AttachmentC_8	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentC_8	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
AttachmentD_1	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentD_1	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
AttachmentE_4	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
AttachmentE_4	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentE_5(d)	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。
AttachmentE_1(a)(b)(d)	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
AttachmentE_1(a)(b)(d)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentE_1(a)(b)(d)	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
AttachmentE_1(a)(b)(d)	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentE_1(a)(b)(d)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
AttachmentE_1(a)(b)(d)	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
AttachmentE_1(a)(b)(d)	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
AttachmentE_1(a)(b)(d)	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentE_1(a)(b)(d)	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
AttachmentE_1(a)(b)(d)	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
AttachmentE_1(a)(b)(d)	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentE_1(a)(b)(d)	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentE_1(a)(b)(d)	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentE_1(a)(b)(d)	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentE_1(a)(b)(d)	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
AttachmentE_1(a)(b)(d)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
AttachmentE_1(a)(b)(d)	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for APRA CPG 234」で入手できます。

アセット管理に関する運用上のベストプラクティス

このコンフォーマンスパックには、アセット管理に基づく AWS Config ルールが含まれています AWS。でサポートされているすべてのマネージドルールのリストについては AWS Config、「AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Asset Management」で入手できます。

の運用のベストプラクティス AWS Backup

このコンフォーマンスパックには、 AWS Backup 内に基づく AWS Config ルールが含まれています AWS。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for AWS Backup」で入手できます。

AWS Identity and Access Management に関する運用上のベストプラクティス

テンプレートは、GitHub の「Operational Best Practices for AWS Identity and Access Management」で入手できます。

AWS Well-Architected フレームワークの信頼性の柱に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Amazon Web Services の Well-Architected フレームワークの信頼性の柱と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、柱の設計原則の 1 つ以上に関連しています。A Well-Architected フレームワークのカテゴリを、複数の Config ルールに関連付けることができます これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-1	サービスクォータと制約はどのように管理するのですか。クラウドベースのワークロードアーキテクチャには、サービスクォータ (サービスの制限とも言います) があります。これらのクォータは、サービスを不正使用されないようにするために、必要以上のリソースを誤ってプロビジョニングすることを防ぎ、API オペレーションのリクエストレートを制限するためのものです。また、光ファイバーケーブルにビットをプッシュダウンできる速度や、物理ディスク上のストレージの量などのリソースの制限もあります。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
REL-1	サービスクォータと制約はどのように管理するのですか。クラウドベースのワークロードアーキテクチャには、サービスクォータ (サービスの制限とも言います) があります。これらのクォータは、サービスを不正使用されないようにするために、必要以上のリソースを誤ってプロビジョニングすることを防ぎ、API オペレーションのリクエストレートを制限するためのものです。また、光ファイバーケーブルにビットをプッシュダウンできる速度や、物理ディスク上のストレージの量などのリソースの制限もあります。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-1	サービスクォータと制約はどのように管理するのですか。クラウドベースのワークロードアーキテクチャには、サービスクォータ (サービスの制限とも言います) があります。これらのクォータは、サービスを不正使用されないようにするために、必要以上のリソースを誤ってプロビジョニングすることを防ぎ、API オペレーションのリクエストレートを制限するためのものです。また、光ファイバーケーブルにビットをプッシュダウンできる速度や、物理ディスク上のストレージの量などのリソースの制限もあります。	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service (Amazon ECS) コンテナで使用できる最大メモリを制限することで、コンテナへの悪意のあるアクセスが発生しても、リソースの使用量が悪用されることはありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-2	ネットワークトポロジはどのように計画するのですか。多くの場合、ワークロードは複数の環境に存在します。その中には、複数のクラウド環境 (パブリックアクセスとプライベートの両方) や、場合によっては既存のデータセンターのインフラストラクチャが含まれます。プランには、システム内およびシステム間の接続性、パブリック IP アドレスの管理、プライベート IP アドレスの管理、ドメイン名の解決といったネットワークの考慮事項が含まれている必要があります。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-2	ネットワークトポロジはどのように計画するのですか。多くの場合、ワークロードは複数の環境に存在します。その中には、複数のクラウド環境 (パブリックアクセスとプライベートの両方) や、場合によっては既存のデータセンターのインフラストラクチャが含まれます。プランには、システム内およびシステム間の接続性、パブリック IP アドレスの管理、プライベート IP アドレスの管理、ドメイン名の解決といったネットワークの考慮事項が含まれている必要があります。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-2	ネットワークトポロジはどのように計画するのですか。多くの場合、ワークロードは複数の環境に存在します。その中には、複数のクラウド環境 (パブリックアクセスとプライベートの両方) や、場合によっては既存のデータセンターのインフラストラクチャが含まれます。プランには、システム内およびシステム間の接続性、パブリック IP アドレスの管理、プライベート IP アドレスの管理、ドメイン名の解決といったネットワークの考慮事項が含まれている必要があります。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-5	障害を軽減または耐えるために、分散システムにおけるインタラクションをどのように設計しますか。分散システムは、サーバーやサービスなどのコンポーネントを相互接続するために通信ネットワークに依存しています。これらのネットワークでデータ損失や遅延が発生しても、ワークロードは確実に動作する必要があります。分散システムのコンポーネントは、他のコンポーネントやワークロードに悪影響を及ぼさない方法で動作する必要があります。これらのベストプラクティスは障害を防ぎ、平均故障間隔 (MTBF) を改善します。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	api-gw-xray-enabled	AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集し、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。X-Ray が を有効にして、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も表示できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk の強化されたヘルスレポートでは、特定された問題の重要度を測定し、調査すべき潜在的な原因を特定するためのステータス記述子が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	ecs-container-insights-enabled	モニタリングは、Amazon Elastic Container Service (ECS) と AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。Container Insights では、問題の迅速な特定と解決に役立つ、コンテナの再起動失敗などの診断情報も提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-6	ワークロードのリソースをどのようにモニタリングするのですか。ログやメトリクスは、ワークロードの状態に関するインサイトを得るための強力なツールです。ログやメトリクスをモニタリングし、しきい値を超えたときや、重要なイベントが発生したときに通知を送信するようにワークロードを設定することができます。モニタリングを行うことで、パフォーマンス低下のしきい値を超えたときや、障害が発生したときにワークロードで認識され、自動的に回復することができます。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-7	需要の変化に対応するためには、どのようにワークロードを設計すればよいですか。スケーラブルなワークロードでは、リソースを自動的に追加または削除することで、任意の時点での需要により合致できる伸縮性を得られます。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-7	需要の変化に対応するためには、どのようにワークロードを設計すればよいですか。スケーラブルなワークロードでは、リソースを自動的に追加または削除することで、任意の時点での需要により合致できる伸縮性を得られます。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-7	需要の変化に対応するためには、どのようにワークロードを設計すればよいですか。スケーラブルなワークロードでは、リソースを自動的に追加または削除することで、任意の時点での需要により合致できる伸縮性を得られます。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-8	どのように変更を実装するのですか。コントロールされた変更は、新しい機能をデプロイするために必要ですが、ワークロードやオペレーティング環境が既知のソフトウェアを実行し、予測可能な方法でパッチや置き換えを行うためにも必要です。これらの変更がコントロールされていない場合、変更による影響を予測したり、変更によって発生する問題に対応することが困難になります。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-8	どのように変更を実装するのですか。コントロールされた変更は、新しい機能をデプロイするために必要ですが、ワークロードやオペレーティング環境が既知のソフトウェアを実行し、予測可能な方法でパッチや置き換えを行うためにも必要です。これらの変更がコントロールされていない場合、変更による影響を予測したり、変更によって発生する問題に対応することが困難になります。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-8	どのように変更を実装するのですか。コントロールされた変更は、新しい機能をデプロイするために必要ですが、ワークロードやオペレーティング環境が既知のソフトウェアを実行し、予測可能な方法でパッチや置き換えを行うためにも必要です。これらの変更がコントロールされていない場合、変更による影響を予測したり、変更によって発生する問題に対応することが困難になります。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-8	どのように変更を実装するのですか。コントロールされた変更は、新しい機能をデプロイするために必要ですが、ワークロードやオペレーティング環境が既知のソフトウェアを実行し、予測可能な方法でパッチや置き換えを行うためにも必要です。これらの変更がコントロールされていない場合、変更による影響を予測したり、変更によって発生する問題に対応することが困難になります。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-9	データのバックアップはどのように行うのですか。データ、アプリケーション、設定をバックアップすると、目標復旧時間 (RTO) や目標復旧時点 (RPO) の要件を満たすことができます。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-10	ワークロードを保護するための障害分離はどのように使用するのですか。障害を分離した境界によって、ワークロード内の障害の影響を限られた数のコンポーネントに限定できます。境界の外部のコンポーネントは、障害の影響を受けません。障害を分離した複数の境界を使用して、ワークロードへの影響を制限することができます。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-10	ワークロードを保護するための障害分離はどのように使用するのですか。障害を分離した境界によって、ワークロード内の障害の影響を限られた数のコンポーネントに限定できます。境界の外部のコンポーネントは、障害の影響を受けません。障害を分離した複数の境界を使用して、ワークロードへの影響を制限することができます。	clb-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-10	ワークロードを保護するための障害分離はどのように使用するのですか。障害を分離した境界によって、ワークロード内の障害の影響を限られた数のコンポーネントに限定できます。境界の外部のコンポーネントは、障害の影響を受けません。障害を分離した複数の境界を使用して、ワークロードへの影響を制限することができます。	elbv2-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-10	ワークロードを保護するための障害分離はどのように使用するのですか。障害を分離した境界によって、ワークロード内の障害の影響を限られた数のコンポーネントに限定できます。境界の外部のコンポーネントは、障害の影響を受けません。障害を分離した複数の境界を使用して、ワークロードへの影響を制限することができます。	lambda-vpc-multi-az-check	AWS Lambda 関数がアカウントの Virtual Private Cloud (VPC) に接続するように設定されている場合は、Lambda AWS 関数を少なくとも 2 つの異なるアベイラビリティーゾーンにデプロイして、単一のゾーンでサービスが中断された場合に関数がイベントを処理できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-10	ワークロードを保護するための障害分離はどのように使用するのですか。障害を分離した境界によって、ワークロード内の障害の影響を限られた数のコンポーネントに限定できます。境界の外部のコンポーネントは、障害の影響を受けません。障害を分離した複数の境界を使用して、ワークロードへの影響を制限することができます。	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) では、高可用性と耐障害性のために少なくとも 3 つのデータノードが必要です。少なくとも 3 つのデータノードを持つ OpenSearch Service ドメインをデプロイすると、ノードに障害が発生した場合のクラスターオペレーションが確実になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-10	ワークロードを保護するための障害分離はどのように使用するのですか。障害を分離した境界によって、ワークロード内の障害の影響を限られた数のコンポーネントに限定できます。境界の外部のコンポーネントは、障害の影響を受けません。障害を分離した複数の境界を使用して、ワークロードへの影響を制限することができます。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
REL-10	ワークロードを保護するための障害分離はどのように使用するのですか。障害を分離した境界によって、ワークロード内の障害の影響を限られた数のコンポーネントに限定できます。境界の外部のコンポーネントは、障害の影響を受けません。障害を分離した複数の境界を使用して、ワークロードへの影響を制限することができます。	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
REL-10	ワークロードを保護するための障害分離はどのように使用するのですか。障害を分離した境界によって、ワークロード内の障害の影響を限られた数のコンポーネントに限定できます。境界の外部のコンポーネントは、障害の影響を受けません。障害を分離した複数の境界を使用して、ワークロードへの影響を制限することができます。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for AWS Well-Architected Reliability Pillar」で入手できます。

AWS Well-Architected フレームワークのセキュリティの柱に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Amazon Web Services の Well-Architected フレームワークのセキュリティの柱と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、柱の設計原則の 1 つ以上に関連しています。A Well-Architected フレームワークのカテゴリを、複数の Config ルールに関連付けることができます これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握してお	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握しておくと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握しておくと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握しておくと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握しておくと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握しておくと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握しておくと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握しておくと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握しておくと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-1	ワークロードを安全に運用するにはどうすればよいですか。ワークロードを安全に運用するためには、セキュリティのすべての領域に包括的なベストプラクティスを適用する必要があります。「運用上の優秀性」で定義された要件とプロセスを組織やワークロードのレベルで作成し、あらゆる領域に適用します。 AWS および業界の推奨事項と脅威インテリジェンスを常に把握しておくと、脅威モデルと統制目標の進化に役立ちます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティ運用を拡張できます。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。ヒューマンアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためのアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。ヒューマンアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためのアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。ヒューマンアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためのアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。ヒューマンアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためのアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。ヒューマンアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためのアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。ヒューマンアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためのアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。ヒューマンアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためのアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。ヒューマンアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためのアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。ヒューマンアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためのアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。人間のアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためにアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。人間のアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためにアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。人間のアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためにアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。人間のアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためにアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。人間のアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためにアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。人間のアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためにアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	secretsmanager-secret-periodic-rotation	このルールにより、 AWS Secrets Manager シークレットで定期的なローテーションが有効になっていることが保証されます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。人間のアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためにアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。人間のアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためにアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-2	人やマシンの ID はどのように管理するのですか。安全な AWS ワークロードを運用する際に管理する必要がある ID には 2 つのタイプがあります。管理とアクセス権の付与が必要な ID のタイプを理解すると、適切な ID に、適切な条件下で適切なリソースにアクセスさせることができます。人間のアイデンティティ: 管理者、デベロッパー、オペレーター、エンドユーザーは、 AWS 環境とアプリケーションにアクセスするためにアイデンティティを必要とします。これらは、組織のメンバー、または共同作業を行う外部ユーザーであり、ウェブブラウザ、クライアントアプリケーション、またはインタラクティブなコマンドラインツールから AWS リソースを操作するユーザーで	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	す。マシン ID: サービスアプリケーション、運用ツール、ワークロードには、データの読み取りなど、 AWS サービスへのリクエストを行うために ID が必要です。これらの ID には、Amazon EC2 インスタンスや AWS Lambda 関数など、AWS 環境で実行されているマシンが含まれます。また、アクセスが必要な外部関係者のマシン ID を管理することもできます。さらに、 AWS 環境にアクセス AWS する必要がある の外部のマシンがある場合もあります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。ワークロードの各コンポーネントやリソースには、管理者、エンドユーザー、またはその他のコンポーネントによるアクセスが必要です。各コンポーネントへのアクセス権のある人とマシンを明確に定義し、適切な ID のタイプと、認証および認可の方法を選択します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。組織内のすべての ID へのアクセスを制限する共通コントロールを確立します。例えば、特定の AWS リージョンへのアクセスを制限したり、オペレーターが中央セキュリティチームに使用される IAM ロールなどの一般的なリソースを削除できないようにしたりできます。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-3	人とマシンのアクセス許可をどのように管理するのですか。パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。このタイプのアクセスを必要とするリソースのみへのパブリックおよびクロスアカウントアクセスを減らします。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケット内のオブジェクトにアクセスした AWS アカウント 情報、IP アドレス、およびイベント時刻が含まれます。
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-4	セキュリティイベントをどのように検出して調査するのですか。ログとメトリクスからイベントをキャプチャして分析し、可視性を得ることができます。ワークロードを保護するため、セキュリティイベントと潜在的な脅威に対するアクションを実行します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	ec2-instance-multiple-eni-check	このルールは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに複数の ENI があるかどうかを確認します。複数の ENI が存在すると、デュアルホームインスタンス (複数のサブネットを持つインスタンス) を引き起こす可能性があります。これにより、ネットワークセキュリティの複雑性が増し、意図しないネットワークパスとアクセスが導入する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-5	ネットワークリソースはどのように保護するのですか。インターネットでもプライベートネットワークでも、何らかの形でネットワークに接続しているワークロードには、外部や内部のネットワークベースの脅威から保護するための複数の防御層が必要です。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ecs-container-insights-enabled	モニタリングは、Amazon Elastic Container Service (ECS) と AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。Container Insights では、問題の迅速な特定と解決に役立つ、コンテナの再起動失敗などの診断情報も提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。 AWS Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 はプラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-instance-multiple-eni-check	このルールは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに複数の ENI があるかどうかを確認します。複数の ENI が存在すると、デュアルホームインスタンス (複数のサブネットを持つインスタンス) を引き起こす可能性があります。これにより、ネットワークセキュリティの複雑性が増し、意図しないネットワークパスとアクセスが導入する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-6	コンピューティングリソースはどのように保護するのですか。ワークロード内のコンピューティングリソースは、外部や内部のネットワークベースの脅威から保護するための複数の防御層を必要とします。コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトに対して暗号化が有効になっていることを確認します。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-8	保管中のデータはどのように保護するのですか。複数のコントロールを実装することで保管中のデータを保護し、不正アクセスや誤操作のリスクを軽減します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SEC-9	転送中のデータはどのように保護するのですか。複数のコントロールを実装して転送中のデータを保護することで、不正アクセスや損失のリスクを軽減します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for AWS Well-Architected Security Pillar」で入手できます。

BCP と DR に関する運用上のベストプラクティス

このコンフォーマンスパックには、BCP と DR に基づく AWS Config ルールが含まれています AWS。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for BCP and DR」で入手できます。

BNM の「RMiT」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、マレーシア国立銀行 (BNM) の技術リスク管理 (RMiT) と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の BNM RMiT コントロールに関連付けられます。BNM の「RMiT」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じる	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクについても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.18	金融機関は、情報の機密性、完全性、認証、承認、および否認防止を保護するため、使用されるテクノロジーに関連する暗号化制御について、適切な注意を払って評価する必要があります。金融機関が独自の暗号化キーを生成していない場合、その金融機関は、暗号化キーを管理するための堅牢なコントロールとプロセスが実施されていることを確認するための適切な措置を講じるものとします。第三者の評価に依存する必要がある場合は、その依存が金融機関のリスク選好と許容範囲に合致するかどうかを検討するものとします。また、暗号化制御をサポートするために必要なシステムリソースや、暗号化されたデータのネットワークトラフィックの可視性が低下するリスクにつ	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	いても、十分に考慮する必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.20	金融機関は、リスクのレベルに応じて、認証機関によって発行された証明書に暗号化のパブリックキーを保存するものとします。これらの顧客に関連する証明書は、認定を受けた認証機関によって発行されるものとします。金融機関は、ユーザー証明書に対応する暗号化のプライベートキーの使用が法的拘束力を持ち、議論の余地がないことを保証するために、それらの証明書を使用する認証および署名プロトコルの実装が、強力な保護の対象となっていることを確認する必要があります。このような証明書の最初の発行とその後の更新は、業界のベストプラクティスおよび適用される法律上/規制上の仕様に合致するものでなければなりません。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.20	金融機関は、リスクのレベルに応じて、認証機関によって発行された証明書に暗号化のパブリックキーを保存するものとします。これらの顧客に関連する証明書は、認定を受けた認証機関によって発行されるものとします。金融機関は、ユーザー証明書に対応する暗号化のプライベートキーの使用が法的拘束力を持ち、議論の余地がないことを保証するために、それらの証明書を使用する認証および署名プロトコルの実装が、強力な保護の対象となっていることを確認する必要があります。このような証明書の最初の発行とその後の更新は、業界のベストプラクティスおよび適用される法律上/規制上の仕様に合致するものでなければなりません。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.27	金融機関は、主要なプロセスとサービスにおける容量の使用率とパフォーマンスを追跡するための、リアルタイムのモニタリングメカニズムを確立する必要があります。これらのモニタリングメカニズムは、管理者にタイムリーかつ実用的なアラートを提供できるものでなければなりません。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.27	金融機関は、主要なプロセスとサービスにおける容量の使用率とパフォーマンスを追跡するための、リアルタイムのモニタリングメカニズムを確立する必要があります。これらのモニタリングメカニズムは、管理者にタイムリーかつ実用的なアラートを提供できるものでなければなりません。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.27	金融機関は、主要なプロセスとサービスにおける容量の使用率とパフォーマンスを追跡するための、リアルタイムのモニタリングメカニズムを確立する必要があります。これらのモニタリングメカニズムは、管理者にタイムリーかつ実用的なアラートを提供できるものでなければなりません。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.27	金融機関は、主要なプロセスとサービスにおける容量の使用率とパフォーマンスを追跡するための、リアルタイムのモニタリングメカニズムを確立する必要があります。これらのモニタリングメカニズムは、管理者にタイムリーかつ実用的なアラートを提供できるものでなければなりません。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.27	金融機関は、主要なプロセスとサービスにおける容量の使用率とパフォーマンスを追跡するための、リアルタイムのモニタリングメカニズムを確立する必要があります。これらのモニタリングメカニズムは、管理者にタイムリーかつ実用的なアラートを提供できるものでなければなりません。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
10.27	金融機関は、主要なプロセスとサービスにおける容量の使用率とパフォーマンスを追跡するための、リアルタイムのモニタリングメカニズムを確立する必要があります。これらのモニタリングメカニズムは、管理者にタイムリーかつ実用的なアラートを提供できるものでなければなりません。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
10.27	金融機関は、主要なプロセスとサービスにおける容量の使用率とパフォーマンスを追跡するための、リアルタイムのモニタリングメカニズムを確立する必要があります。これらのモニタリングメカニズムは、管理者にタイムリーかつ実用的なアラートを提供できるものでなければなりません。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.27	金融機関は、主要なプロセスとサービスにおける容量の使用率とパフォーマンスを追跡するための、リアルタイムのモニタリングメカニズムを確立する必要があります。これらのモニタリングメカニズムは、管理者にタイムリーかつ実用的なアラートを提供できるものでなければなりません。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.27	金融機関は、主要なプロセスとサービスにおける容量の使用率とパフォーマンスを追跡するための、リアルタイムのモニタリングメカニズムを確立する必要があります。これらのモニタリングメカニズムは、管理者にタイムリーかつ実用的なアラートを提供できるものでなければなりません。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.34	金融機関は、潜在的なネットワーク障害やサイバー脅威から重要なシステムを保護するために、重要なシステム向けのネットワークサービスの信頼性を確保し、SPOF が存在しないことを確認する必要があります。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.34	金融機関は、潜在的なネットワーク障害やサイバー脅威から重要なシステムを保護するために、重要なシステム向けのネットワークサービスの信頼性を確保し、SPOF が存在しないことを確認する必要があります。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.35	金融機関は、ネットワーク帯域幅のリアルタイムのモニタリングプロセスと、対応するネットワークサービスの回復性のメトリクスを確立し、帯域幅の過剰な使用率、帯域幅の輻輳、ネットワーク障害によるシステムの中断にフラグを付けられるようにする必要があります。これには、傾向や異常を検出するためのトラフィック分析が含まれます。	api-gw-xray-enabled	AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集し、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。X-Ray が を有効にして、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も表示できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.35	金融機関は、ネットワーク帯域幅のリアルタイムのモニタリングプロセスと、対応するネットワークサービスの回復性のメトリクスを確立し、帯域幅の過剰な使用率、帯域幅の輻輳、ネットワーク障害によるシステムの中断にフラグを付けられるようにする必要があります。これには、傾向や異常を検出するためのトラフィック分析が含まれます。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.35	金融機関は、ネットワーク帯域幅のリアルタイムのモニタリングプロセスと、対応するネットワークサービスの回復性のメトリクスを確立し、帯域幅の過剰な使用率、帯域幅の輻輳、ネットワーク障害によるシステムの中断にフラグを付けられるようにする必要があります。これには、傾向や異常を検出するためのトラフィック分析が含まれます。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.35	金融機関は、ネットワーク帯域幅のリアルタイムのモニタリングプロセスと、対応するネットワークサービスの回復性のメトリクスを確立し、帯域幅の過剰な使用率、帯域幅の輻輳、ネットワーク障害によるシステムの中断にフラグを付けられるようにする必要があります。これには、傾向や異常を検出するためのトラフィック分析が含まれます。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
10.36	金融機関は、重要なシステムをサポートするネットワークサービスが、データの機密性、整合性、可用性を確保するように設計および実装されていることを確認する必要があります。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.36	金融機関は、重要なシステムをサポートするネットワークサービスが、データの機密性、整合性、可用性を確保するように設計および実装されていることを確認する必要があります。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
10.36	金融機関は、重要なシステムをサポートするネットワークサービスが、データの機密性、整合性、可用性を確保するように設計および実装されていることを確認する必要があります。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.36	金融機関は、重要なシステムをサポートするネットワークサービスが、データの機密性、整合性、可用性を確保するように設計および実装されていることを確認する必要があります。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
10.36	金融機関は、重要なシステムをサポートするネットワークサービスが、データの機密性、整合性、可用性を確保するように設計および実装されていることを確認する必要があります。	nlb-cross-zone-load-balancing-enabled	Network Load Balancer (NLB) のクロスゾーンロードバランサーを有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.38	金融機関は、調査と法律上の目的で、関連する十分なネットワークデバイスログを、少なくとも 3 年間、保持する必要があります。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.51	金融機関がクラウドサービスを利用する際は、不正な開示やアクセスから保護するために、顧客や取引先の情報や所有権のあるデータに対して適切な保護措置を講じる必要があります。これには、クラウド上でホストされている顧客や取引先の情報、所有権のあるデータやサービスに関連するすべてのデータの所有権、コントロール、管理の保持を含むものとし、関連する暗号化キーの管理も含まれるものとします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.52	金融機関は、ユーザー (サードパーティーのサービスプロバイダーなどの内部と外部のユーザー) の識別、認証、承認のための適切なアクセスコントロールポリシーを実装する必要があります。これは、テクノロジーやシステムへの不正アクセスのリスクレベルに見合っており、アクセスコントロールに論理的かつ物理的なテクノロジーで対応するものでなければなりません	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(b)(h)(i)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて以下の原則を考慮する必要があります。(b) 「最小特権」のアクセス許可を採用するか、「需要」ベースで正当なユーザに、そのロールを実行するための必要最低限の権限のみを付与する。(h) 複数のユーザ間でのユーザ ID およびパスワードの共有を制限および管理する。(i) より個人を特定しやすい ID を優先し、一般的なユーザー ID の命名規則の使用を管理する。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(b)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて、以下の原則を考慮する必要があります。(b) 「最小特権」のアクセス許可を採用するか、「需要」ベースで、正当なユーザに、そのロールを実行するための必要最低限の権限のみを付与する。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(b)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて、以下の原則を考慮する必要があります。(b) 「最小特権」のアクセス許可を採用するか、「需要」ベースで、正当なユーザに、そのロールを実行するための必要最低限の権限のみを付与する。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(b)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて、以下の原則を考慮する必要があります。(b) 「最小特権」のアクセス許可を採用するか、「需要」ベースで、正当なユーザに、そのロールを実行するための必要最低限の権限のみを付与する。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(b)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて、以下の原則を考慮する必要があります。(b) 「最小特権」のアクセス許可を採用するか、「需要」ベースで、正当なユーザに、そのロールを実行するための必要最低限の権限のみを付与する。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(b)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて、以下の原則を考慮する必要があります。(b) 「最小特権」のアクセス許可を採用するか、「需要」ベースで、正当なユーザに、そのロールを実行するための必要最低限の権限のみを付与する。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(b)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて、以下の原則を考慮する必要があります。(b) 「最小特権」のアクセス許可を採用するか、「需要」ベースで、正当なユーザに、そのロールを実行するための必要最低限の権限のみを付与する。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
10.53(b)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて、以下の原則を考慮する必要があります。(b) 「最小特権」のアクセス許可を採用するか、「需要」ベースで、正当なユーザに、そのロールを実行するための必要最低限の権限のみを付与する。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(c)(f)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて以下の原則を考慮する必要があります。(c) サービスプロバイダーに付与されたアクセス許可を含む、特定の期間にアクセスを制限する期限付きのアクセス権現を採用する。(f) リモートアクセスを含む重要なアクティビティに対し、より強力な認証を採用する。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
10.53(f)(h)	10.52 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて以下の原則を考慮する必要があります。(f) リモートアクセスを含む重要なアクティビティに対する、より強力な認証を採用する。(h) 複数のユーザー間でのユーザー ID とパスワードの共有を制限および制御する。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(f)(h)	10.54 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて以下の原則を考慮する必要があります。(f) リモートアクセスを含む重要なアクティビティに対する、より強力な認証を採用する。(h) 複数のユーザー間でのユーザー ID とパスワードの共有を制限および制御する。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.53(f)(h)	10.54 項を遵守するにあたり、金融機関はアクセスコントロールポリシーにおいて以下の原則を考慮する必要があります。(f) リモートアクセスを含む重要なアクティビティに対する、より強力な認証を採用する。(h) 複数のユーザー間でのユーザー ID とパスワードの共有を制限および制御する。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.54	金融機関は、使用中の ID の信頼性を確保するため、堅牢な認証プロセスを採用する必要があります。認証メカニズムには、機能の重要性に応じて、ユーザーが記憶するもの (パスワードや PIN など)、ユーザーが所有するもの (スマートカードやセキュリティデバイスなど)、ユーザー自身 (指紋や網膜パターンなどのバイオメトリクス特性など) といった 3 つの基本的な認証要素のうち、少なくとも 1 つ以上を採用するものとします。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.54	金融機関は、使用中の ID の信頼性を確保するため、堅牢な認証プロセスを採用する必要があります。認証メカニズムには、機能の重要性に応じて、ユーザーが記憶するもの (パスワードや PIN など)、ユーザーが所有するもの (スマートカードやセキュリティデバイスなど)、ユーザー自身 (指紋や網膜パターンなどのバイオメトリクス特性など) といった 3 つの基本的な認証要素のうち、少なくとも 1 つ以上を採用するものとします。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.54	金融機関は、使用中の ID の信頼性を確保するため、堅牢な認証プロセスを採用する必要があります。認証メカニズムには、機能の重要性に応じて、ユーザーが記憶するもの (パスワードや PIN など)、ユーザーが所有するもの (スマートカードやセキュリティデバイスなど)、ユーザー自身 (指紋や網膜パターンなどのバイオメトリクス特性など) といった 3 つの基本的な認証要素のうち、少なくとも 1 つ以上を採用するものとします。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.55	金融機関は、進化する攻撃に対する回復性を強化するために、パスワードの使用方法を定期的に見直し、改変するものとします。これには、効果的で安全なパスワードの生成が含まれます。作成したパスワードの強度をチェックするためには、適切な管理を行う必要があります。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
10.56	複数の要素を使用する認証方法は、一般的に、単一の要素を使用するシステムよりも侵害されにくくなります。このことから、金融機関では (特に、高リスクのシステムや「シングルサインオン」を使用するシステムにおいて)、より信頼性が高く、より強力な不正の抑止力となる多要素認証 (MFA) を適切に設計し、実装することが推奨されます	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.56	複数の要素を使用する認証方法は、一般的に、単一の要素を使用するシステムよりも侵害されにくくなります。このことから、金融機関では (特に、高リスクのシステムや「シングルサインオン」を使用するシステムにおいて)、より信頼性が高く、より強力な不正の抑止力となる多要素認証 (MFA) を適切に設計し、実装することが推奨されます	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.56	複数の要素を使用する認証方法は、一般的に、単一の要素を使用するシステムよりも侵害されにくくなります。このことから、金融機関では (特に、高リスクのシステムや「シングルサインオン」を使用するシステムにおいて)、より信頼性が高く、より強力な不正の抑止力となる多要素認証 (MFA) を適切に設計し、実装することが推奨されます	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.59	金融機関は、以下のことを確認する必要があります。(a) 企業全体のシステムへのアクセスコントロールが効果的に管理および監視されている。(b) 重要なシステムでのユーザーアクティビティが、監査と調査のためにログに記録されている。アクティビティログは最低 3 年間保存し、定期的かつタイムリーに確認する必要があります。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.60	10.59 項の要件を満たす上で、大規模な金融機関では以下のことを行う必要があります。(a) 企業全体のシステムへのユーザーアクセスを効果的に管理およびモニタリングするための ID のアクセス管理システムをデプロイする。(b) 自動監査ツールをデプロイし、あらゆる異常にフラグを付ける。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
10.60	10.61 項の要件を満たす上で、大規模な金融機関では以下のことを行う必要があります。(a) 企業全体のシステムへのユーザーアクセスを効果的に管理およびモニタリングするための ID のアクセス管理システムをデプロイする。(b) 自動監査ツールをデプロイし、あらゆる異常にフラグを付ける。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.60	10.61 項の要件を満たす上で、大規模な金融機関では以下のことを行う必要があります。(a) 企業全体のシステムへのユーザーアクセスを効果的に管理およびモニタリングするための ID のアクセス管理システムをデプロイする。(b) 自動監査ツールをデプロイし、あらゆる異常にフラグを付ける。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.61	金融機関は、重要なシステムが、セキュリティの脆弱性が明らかになっている古いシステムや、サポートの終了した (EOL) テクノロジーを使用したシステム上で稼働していないことを確認する必要があります。その際、金融機関は特定された機能に対して、明確に責任を割り当てる必要があります。(a) 最新のパッチリリースをタイムリーかつ継続的にモニタリングおよび実装します。(b) さらなる是正措置を実行するために、EOL に近づいている重要なテクノロジーを使用するシステムを特定します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.61	金融機関は、重要なシステムが、セキュリティの脆弱性が明らかになっている古いシステムや、サポートの終了した (EOL) テクノロジーを使用したシステム上で稼働していないことを確認する必要があります。その際、金融機関は特定された機能に対して、明確に責任を割り当てる必要があります。(a) 最新のパッチリリースをタイムリーかつ継続的にモニタリングおよび実装します。(b) さらなる是正措置を実行するために、EOL に近づいている重要なテクノロジーを使用するシステムを特定します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.61	金融機関は、重要なシステムが、セキュリティの脆弱性が明らかになっている古いシステムや、サポートの終了した (EOL) テクノロジーを使用したシステム上で稼働していないことを確認する必要があります。その際、金融機関は特定された機能に対して、明確に責任を割り当てる必要があります。(a) 最新のパッチリリースをタイムリーかつ継続的にモニタリングおよび実装します。(b) さらなる是正措置を実行するために、EOL に近づいている重要なテクノロジーを使用するシステムを特定します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.61	金融機関は、重要なシステムが、セキュリティの脆弱性が明らかになっている古いシステムや、サポートの終了した (EOL) テクノロジーを使用したシステム上で稼働していないことを確認する必要があります。その際、金融機関は特定された機能に対して、明確に責任を割り当てる必要があります。(a) 最新のパッチリリースをタイムリーかつ継続的にモニタリングおよび実装します。(b) さらなる是正措置を実行するために、EOL に近づいている重要なテクノロジーを使用するシステムを特定します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.61	金融機関は、重要なシステムが、セキュリティの脆弱性が明らかになっている古いシステムや、サポートの終了した (EOL) テクノロジーを使用したシステム上で稼働していないことを確認する必要があります。その際、金融機関は特定された機能に対して、明確に責任を割り当てる必要があります。(a) 最新のパッチリリースをタイムリーかつ継続的にモニタリングおよび実装します。(b) さらなる是正措置を実行するために、EOL に近づいている重要なテクノロジーを使用するシステムを特定します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.64(a)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実装する必要があります。(a) 顧客および取引先の情報と、トランザクションの機密性および完全性	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(b)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(b) チャネルやデバイスから、サービスの中断を最小限に抑えて提供されるサービスの信頼性	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(b)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(b) チャネルやデバイスから、サービスの中断を最小限に抑えて提供されるサービスの信頼性	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
10.64(b)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(b) チャネルやデバイスから、サービスの中断を最小限に抑えて提供されるサービスの信頼性	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(b)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(b) チャネルやデバイスから、サービスの中断を最小限に抑えて提供されるサービスの信頼性	nlb-cross-zone-load-balancing-enabled	NetworkLoad Balancer (NLB) のクロスゾーンロードバランシングを有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
10.64(b)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(b) チャネルやデバイスから、サービスの中断を最小限に抑えて提供されるサービスの信頼性	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(b)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(b) チャネルやデバイスから、サービスの中断を最小限に抑えて提供されるサービスの信頼性	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(b)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(b) チャネルやデバイスから、サービスの中断を最小限に抑えて提供されるサービスの信頼性	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
10.64(b)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(b) チャネルやデバイスから、サービスの中断を最小限に抑えて提供されるサービスの信頼性	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(d)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(d) 十分な監査証跡と異常なトランザクションのモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.64(e)	金融機関は、デジタルサービスを提供する際、以下のことを保証する堅牢なテクノロジーによるセキュリティコントロールを実施する必要があります。(e) インシデントやサービス中断の前にリカバリポイントを特定して復旧させる機能	s3-resources-protected-by-backup-plan	データのバックアッププロセスを支援するために、Amazon Simple Storage Service (S3) バケットが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.7	金融機関は、テクノロジーインフラストラクチャの異常なアクティビティを継続的かつプロアクティブにモニタリングし、タイムリーに検出するための効果的なツールをデプロイする必要があります。モニタリングの範囲は、サポートするインフラストラクチャを含むあらゆる重要なシステムをカバーする必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.7	金融機関は、テクノロジーインフラストラクチャの異常なアクティビティを継続的かつプロアクティブにモニタリングし、タイムリーに検出するための効果的なツールをデプロイする必要があります。モニタリングの範囲は、サポートするインフラストラクチャを含むあらゆる重要なシステムをカバーする必要があります。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.8	金融機関は、サイバーセキュリティオペレーションによって、セキュリティ管理への潜在的な侵害やセキュリティ体制の弱体化を、継続的に防止および検出する必要があります。大規模な金融機関では、すべての重要なシステムをサポートする外部および内部のネットワークコンポーネントに対して、四半期ごとに脆弱性評価を行う必要もあります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.8	金融機関は、サイバーセキュリティオペレーションによって、セキュリティ管理への潜在的な侵害やセキュリティ体制の弱体化を、継続的に防止および検出する必要があります。大規模な金融機関では、すべての重要なシステムをサポートする外部および内部のネットワークコンポーネントに対して、四半期ごとに脆弱性評価を行う必要もあります。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.18(c)(f)	SOC は、以下の機能を実行可能である必要があります。(c) 脆弱性管理。(f) 脅威インテリジェンスの分析と運用を含む、攻撃者と脅威を検出するための状況認識の提供、および侵入の痕跡 (IOC) のモニタリング。これには、署名のないマルウェアやファイルのないマルウェアを検出し、エンドポイントやネットワークレイヤーなどでセキュリティ脅威となりうる異常を特定するための高度な動作分析が含まれます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.18(c)(f)	SOC は、以下の機能を実行可能である必要があります。(c) 脆弱性管理。(f) 脅威インテリジェンスの分析と運用を含む、攻撃者と脅威を検出するための状況認識の提供、および侵入の痕跡 (IOC) のモニタリング。これには、署名のないマルウェアやファイルのないマルウェアを検出し、エンドポイントやネットワークレイヤーなどでセキュリティ脅威となりうる異常を特定するための高度な動作分析が含まれます。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.18(c)(f)	SOC は、以下の機能を実行可能である必要があります。(c) 脆弱性管理。(f) 脅威インテリジェンスの分析と運用を含む、攻撃者と脅威を検出するための状況認識の提供、および侵入の痕跡 (IOC) のモニタリング。これには、署名のないマルウェアやファイルのないマルウェアを検出し、エンドポイントやネットワークレイヤーなどでセキュリティ脅威となりうる異常を特定するための高度な動作分析が含まれます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.1	すべてのセキュリティデバイスの設定およびルール設定を定期的に確認します。自動化ツールを使用して、設定およびルール設定の変更を確認し、モニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.1	すべてのセキュリティデバイスの設定およびルール設定を定期的に確認します。自動化ツールを使用して、設定およびルール設定の変更を確認し、モニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.5 (b)	サーバー間の外部ネットワーク接続に、以下のセキュリティコントロールが含まれていることを確認します。(b) Transport Layer Security (TLS) やバーチャルプライベートネットワーク (VPN) IPSec などの安全なトンネルの使用。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
付録 5.5 (b)	サーバー間の外部ネットワーク接続に、以下のセキュリティコントロールが含まれていることを確認します。(b) Transport Layer Security (TLS) やバーチャルプライベートネットワーク (VPN) IPSec などの安全なトンネルの使用。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.5 (b)	サーバー間の外部ネットワーク接続に、以下のセキュリティコントロールが含まれていることを確認します。(b) Transport Layer Security (TLS) やバーチャルプライベートネットワーク (VPN) IPSec などの安全なトンネルの使用。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
付録 5.5 (b)	サーバー間の外部ネットワーク接続に、以下のセキュリティコントロールが含まれていることを確認します。(b) Transport Layer Security (TLS) やバーチャルプライベートネットワーク (VPN) IPSec などの安全なトンネルの使用。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.5 (b)	サーバー間の外部ネットワーク接続に、以下のセキュリティコントロールが含まれていることを確認します。(b) Transport Layer Security (TLS) やバーチャルプライベートネットワーク (VPN) IPSec などの安全なトンネルの使用。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
付録 5.5 (b)	サーバー間の外部ネットワーク接続に、以下のセキュリティコントロールが含まれていることを確認します。(b) Transport Layer Security (TLS) やバーチャルプライベートネットワーク (VPN) IPSec などの安全なトンネルの使用。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.5 (c)	サーバー間の外部ネットワーク接続に、以下のセキュリティコントロールが含まれていることを確認します。(c) ファイアウォール、IPS、ウイルス対策など、適切な境界防御と保護を備えたステージングサーバーをデプロイする。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.5 (c)	サーバー間の外部ネットワーク接続に、以下のセキュリティコントロールが含まれていることを確認します。(c) ファイアウォール、IPS、ウイルス対策など、適切な境界防御と保護を備えたステージングサーバーをデプロイする。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.5 (c)	サーバー間の外部ネットワーク接続に、以下のセキュリティコントロールが含まれていることを確認します。(c) ファイアウォール、IPS、ウイルス対策など、適切な境界防御と保護を備えたステージングサーバーをデプロイする。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.6	サーバーへのリモートアクセスに、以下のセキュリティコントロールが含まれていることを確認します。(a) 強化され、ロックダウンされたエンドポイントのデバイスのみにアクセスを制限する。(b) TLS や VPN IPSec などの安全なトンネルを使用する。(c) ファイアウォール、IPS、ウイルス対策などの適切な境界防御と保護を備えた「ゲートウェイ」サーバーをデプロイする。(d) リモートアクセスの有効期限が切れたら、すぐに関連するポートを閉じる。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.6	サーバーへのリモートアクセスに、以下のセキュリティコントロールが含まれていることを確認します。(a) 強化され、ロックダウンされたエンドポイントのデバイスのみにアクセスを制限する。(b) TLS や VPN IPSec などの安全なトンネルを使用する。(c) ファイアウォール、IPS、ウイルス対策などの適切な境界防御と保護を備えた「ゲートウェイ」サーバーをデプロイする。(d) リモートアクセスの有効期限が切れたら、すぐに関連するポートを閉じる。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.6	サーバーへのリモートアクセスに、以下のセキュリティコントロールが含まれていることを確認します。(a) 強化され、ロックダウンされたエンドポイントのデバイスのみにアクセスを制限する。(b) TLS や VPN IPSec などの安全なトンネルを使用する。(c) ファイアウォール、IPS、ウイルス対策などの適切な境界防御と保護を備えた「ゲートウェイ」サーバーをデプロイする。(d) リモートアクセスの有効期限が切れたら、すぐに関連するポートを閉じる。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.6	サーバーへのリモートアクセスに、以下のセキュリティコントロールが含まれていることを確認します。(a) 強化され、ロックダウンされたエンドポイントのデバイスのみにアクセスを制限する。(b) TLS や VPN IPSec などの安全なトンネルを使用する。(c) ファイアウォール、IPS、ウイルス対策などの適切な境界防御と保護を備えた「ゲートウェイ」サーバーをデプロイする。(d) リモートアクセスの有効期限が切れたら、すぐに関連するポートを閉じる。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.6	サーバーへのリモートアクセスに、以下のセキュリティコントロールが含まれていることを確認します。(a) 強化され、ロックダウンされたエンドポイントのデバイスのみにアクセスを制限する。(b) TLS や VPN IPSec などの安全なトンネルを使用する。(c) ファイアウォール、IPS、ウイルス対策などの適切な境界防御と保護を備えた「ゲートウェイ」サーバーをデプロイする。(d) リモートアクセスの有効期限が切れたら、すぐに関連するポートを閉じる。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 5.6	サーバーへのリモートアクセスに、以下のセキュリティコントロールが含まれていることを確認します。(a) 強化され、ロックダウンされたエンドポイントのデバイスのみにアクセスを制限する。(b) TLS や VPN IPSec などの安全なトンネルを使用する。(c) ファイアウォール、IPS、ウイルス対策などの適切な境界防御と保護を備えた「ゲートウェイ」サーバーをデプロイする。(d) リモートアクセスの有効期限が切れたら、すぐに関連するポートを閉じる。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (a)	金融機関は、堅牢なクラウドアーキテクチャを設計し、その設計が想定するアプリケーションに関連する国際規格に準拠していることを確認する必要があります。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
付録 10 パート B - 1 (b)	金融機関は、「違反を想定する」という考え方を採用し、マイクロセグメンテーション、「デフォルトによる拒否」、「最小特権」のアクセス権限を通して多層防御を重ね、該当する場合は詳細な検査と継続的な検証を実施することにより、サイバーレジリエントなアーキテクチャを実現するためにゼロトラストの原則を採用することをお勧めします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (b)	金融機関は、「違反を想定する」という考え方を採用し、マイクロセグメンテーション、「デフォルトによる拒否」、「最小特権」のアクセス権限を通して多層防御を重ね、該当する場合は詳細な検査と継続的な検証を実施することにより、サイバーレジリエントなアーキテクチャを実現するためにゼロトラストの原則を採用することをお勧めします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (b)	金融機関は、「違反を想定する」という考え方を採用し、マイクロセグメンテーション、「デフォルトによる拒否」、「最小特権」のアクセス権限を通して多層防御を重ね、該当する場合は詳細な検査と継続的な検証を実施することにより、サイバーレジリエントなアーキテクチャを実現するためにゼロトラストの原則を採用することをお勧めします。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (b)	金融機関は、「違反を想定する」という考え方を採用し、マイクロセグメンテーション、「デフォルトによる拒否」、「最小特権」のアクセス権限を通して多層防御を重ね、該当する場合は詳細な検査と継続的な検証を実施することにより、サイバーレジリエントなアーキテクチャを実現するためにゼロトラストの原則を採用することをお勧めします。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (c)	金融機関は、複雑なクラウドネットワーク環境の管理において、きめ細かなネットワークセキュリティと集中型ネットワークプロビジョニングを管理およびモニタリングするために、最新のネットワークアーキテクチャアプローチ、適切なネットワーク設計概念とソリューションを使用する必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (c)	金融機関は、複雑なクラウドネットワーク環境の管理において、きめ細かなネットワークセキュリティと集中型ネットワークプロビジョニングを管理およびモニタリングするために、最新のネットワークアーキテクチャアプローチ、適切なネットワーク設計概念とソリューションを使用する必要があります。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
付録 10 パート B - 1 (d)	金融機関は、物理サーバー、アプリケーション、またはデータをクラウドプラットフォームに移行するために、安全で暗号化された通信チャネルを確立し、利用する必要があります。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (d)	金融機関は、物理サーバー、アプリケーション、またはデータをクラウドプラットフォームに移行するために、安全で暗号化された通信チャネルを確立し、利用する必要があります。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (f) i)	金融機関が外部のアプリケーションサービスプロバイダーと相互接続するためにアプリケーションプログラミングインターフェイス (API) の使用が増加することにより、新しいサービス配信の効率を高めることができる可能性があります。ただし、これによりサイバーアタックサーフェスが増加し、管理の誤りによって情報セキュリティインシデントの影響を増幅させる可能性があります。金融機関は、API が次を含む厳格な管理および制御メカニズムの対象となるようにする必要があります。i) API は、単一障害点のリスクを回避するためにサービスの耐障害性を考慮して設計され、適切なアクセス制御により安全に設定されている必要があります。	api-gwv2-authorization-type-configured	Amazon API Gateway v2 API ルートは、基盤となるバックエンドリソースへの不正なアクセスを防ぐために認可タイプが設定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (f) ii)	金融機関が外部のアプリケーションサービスプロバイダーと相互接続するためにアプリケーションプログラミングインターフェイス (API) の使用が増加することにより、新しいサービス配信の効率を高めることができる可能性があります。ただし、これによりサイバーアタックサーフェスが増加し、管理の誤りによって情報セキュリティインシデントの影響を増幅させる可能性があります。金融機関は、API が次を含む厳格な管理および制御メカニズムの対象となるようにする必要があります。ii) API は、適切なインシデント対応策によりサイバー攻撃に対する追跡およびモニタリングを行い、使用されなくなった場合は適時に停止する必要があります。	[api-gw-associated-with-waf](https://aws.amazon.com/)	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 1 (f) ii)	金融機関が外部のアプリケーションサービスプロバイダーと相互接続するためにアプリケーションプログラミングインターフェイス (API) の使用が増加することにより、新しいサービス配信の効率を高めることができる可能性があります。ただし、これによりサイバーアタックサーフェスが増加し、管理の誤りによって情報セキュリティインシデントの影響を増幅させる可能性があります。金融機関は、API が次を含む厳格な管理および制御メカニズムの対象となるようにする必要があります。ii) API は、適切なインシデント対応策によりサイバー攻撃に対する追跡およびモニタリングを行い、使用されなくなった場合は適時に停止する必要があります。	[api-gw-execution-logging-enabled](#)	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 2 (b) ii)	金融機関は、強化されたクラウド機能を継続的に活用してクラウドサービスのセキュリティを向上させる必要があります。また、金融機関にはとりわけ次をお勧めします。ii) サービスのデプロイに不変のインフラストラクチャプラクティスを使用し、最新の安定したバージョンのソフトウェアを使用した新しい環境を作成することにより障害のリスクを軽減します。クラウド環境で進行中のモニタリングには、コンプライアンスレビューを改善し、進化し続けるサイバー攻撃と戦うために、変更不可能なインフラストラクチャへの変更の検出を自動化することが含まれている必要があります。	cloudformation-stack-notification-check	基盤となる AWS リソースへの意図しない変更を検出するには、CloudFormation スタックが Amazon SNS トピックにイベント通知を送信するように設定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 3 (b) vi)	金融機関は、仮想マシンとコンテナイメージが適切に設定、強化、モニタリングされていることを確認する必要があります。これには次が含まれます。vi) 保存されたイメージが、不正アクセスや変更によるセキュリティモニタリングの対象となります。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (a) i)	効果的な復旧能力の一部として、金融機関は既存のバックアップと復旧の手順をクラウドサービスもカバーできるように拡張しておく必要があります。これには次が含まれます。i) クラウド導入の計画段階で、バックアップと復旧戦略を定義し、形式化する。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (a) i)	効果的な復旧能力の一部として、金融機関は既存のバックアップと復旧の手順をクラウドサービスもカバーできるように拡張しておく必要があります。これには次が含まれます。i) クラウド導入の計画段階で、バックアップと復旧戦略を定義し、形式化する。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (a) i)	効果的な復旧能力の一部として、金融機関は既存のバックアップと復旧の手順をクラウドサービスもカバーできるように拡張しておく必要があります。これには次が含まれます。i) クラウド導入の計画段階で、バックアップと復旧戦略を定義し、形式化する。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (a) i)	効果的な復旧能力の一部として、金融機関は既存のバックアップと復旧の手順をクラウドサービスもカバーできるように拡張しておく必要があります。これには次が含まれます。i) クラウド導入の計画段階で、バックアップと復旧戦略を定義し、形式化する。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (a) i)	効果的な復旧能力の一部として、金融機関は既存のバックアップと復旧の手順をクラウドサービスもカバーできるように拡張しておく必要があります。これには次が含まれます。i) クラウド導入の計画段階で、バックアップと復旧戦略を定義し、形式化する。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (a) i)	効果的な復旧能力の一部として、金融機関は既存のバックアップと復旧の手順をクラウドサービスもカバーできるように拡張しておく必要があります。これには次が含まれます。i) クラウド導入の計画段階で、バックアップと復旧戦略を定義し、形式化する。	s3-resources-protected-by-backup-plan	データのバックアッププロセスを支援するために、Amazon Simple Storage Service (S3) バケットが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (b)	金融機関は、バックアップと復元の手順を定期的にテストして、復旧機能を検証する必要があります。バックアップ手順の頻度は、システムの重大度とシステムの目標復旧時点 (RPO) に比例している必要があります。バックアップに失敗した場合、金融機関は迅速に是正措置を実行する必要があります。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (c) i)	金融機関は、バックアップ設定 (該当する場合、IaaS および PaaS 用) を含め、仮想マシンおよびコンテナの十分なバックアップとリカバリを確保する必要があります。これには、次が含まれます。i)ビジネスリカバリの目標によって指定された通り、仮想マシンおよびコンテナを特定の時点で復元する機能を確認する。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
付録 10 パート B - 5 (d) i)	金融機関は、クラウドサービスの耐障害性要件を評価し、システムの重大性に見合った適切な措置を特定して、極端に有害なシナリオでもサービスの可用性を確保する必要があります。金融機関は、サービスの可用性を確保し、集中リスクを軽減するために、リスクベースのアプローチを検討し、適切な緩和策を段階的に採用する必要があります。実行可能なオプションとしては、クラウドサービスの高可用性と冗長性を活用して、運用データセンターのキャパシティを異なるアベイラビリティーゾーンで確実に冗長化できるようにすることなどが挙げられます。	autoscaling-multiple-az	高可用性を確保するには、Auto Scaling グループが複数のアベイラビリティーゾーンの範囲にまたがって設定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (d) i)	金融機関は、クラウドサービスの耐障害性要件を評価し、システムの重大性に見合った適切な措置を特定して、極端に有害なシナリオでもサービスの可用性を確保する必要があります。金融機関は、サービスの可用性を確保し、集中リスクを軽減するために、リスクベースのアプローチを検討し、適切な緩和策を段階的に採用する必要があります。実行可能なオプションとしては、クラウドサービスの高可用性と冗長性を活用して、運用データセンターのキャパシティを異なるアベイラビリティーゾーンで確実に冗長化できるようにすることなどが挙げられます。	elbv2-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (d) i)	金融機関は、クラウドサービスの耐障害性要件を評価し、システムの重大性に見合った適切な措置を特定して、極端に有害なシナリオでもサービスの可用性を確保する必要があります。金融機関は、サービスの可用性を確保し、集中リスクを軽減するために、リスクベースのアプローチを検討し、適切な緩和策を段階的に採用する必要があります。実行可能なオプションとしては、クラウドサービスの高可用性と冗長性を活用して、運用データセンターのキャパシティを異なるアベイラビリティーゾーンで確実に冗長化できるようにすることなどが挙げられます。	lambda-vpc-multi-az-check	AWS Lambda 関数がアカウントの Virtual Private Cloud (VPC) に接続するように設定されている場合は、Lambda AWS 関数を少なくとも 2 つの異なるアベイラビリティーゾーンにデプロイして、単一のゾーンでサービスが中断された場合に関数がイベントを処理できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (d) i)	金融機関は、クラウドサービスの耐障害性要件を評価し、システムの重大性に見合った適切な措置を特定して、極端に有害なシナリオでもサービスの可用性を確保する必要があります。金融機関は、サービスの可用性を確保し、集中リスクを軽減するために、リスクベースのアプローチを検討し、適切な緩和策を段階的に採用する必要があります。実行可能なオプションとしては、クラウドサービスの高可用性と冗長性を活用して、運用データセンターのキャパシティを異なるアベイラビリティーゾーンで確実に冗長化できるようにすることなどが挙げられます。	nlb-cross-zone-load-balancing-enabled	NetworkLoad Balancer (NLB) のクロスゾーンロードバランシングを有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (d) i)	金融機関は、クラウドサービスの耐障害性要件を評価し、システムの重大性に見合った適切な措置を特定して、極端に有害なシナリオでもサービスの可用性を確保する必要があります。金融機関は、サービスの可用性を確保し、集中リスクを軽減するために、リスクベースのアプローチを検討し、適切な緩和策を段階的に採用する必要があります。実行可能なオプションとしては、クラウドサービスの高可用性と冗長性を活用して、運用データセンターのキャパシティを異なるアベイラビリティーゾーンで確実に冗長化できるようにすることなどが挙げられます。	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 5 (d) i)	金融機関は、クラウドサービスの耐障害性要件を評価し、システムの重大性に見合った適切な措置を特定して、極端に有害なシナリオでもサービスの可用性を確保する必要があります。金融機関は、サービスの可用性を確保し、集中リスクを軽減するために、リスクベースのアプローチを検討し、適切な緩和策を段階的に採用する必要があります。実行可能なオプションとしては、クラウドサービスの高可用性と冗長性を活用して、運用データセンターのキャパシティを異なるアベイラビリティーゾーンで確実に冗長化できるようにすることなどが挙げられます。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	eks-secrets-encrypted	保管中のデータを保護するため、Amazon Elastic Kubernetes Service (EKS) クラスターが Kubernetes シークレットを暗号化するように設定されていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
付録 10 パート B - 8 (a)	金融機関は、クラウドに保存されている機密データの機密性と整合性を保護するために、適切で関連する暗号化技術を実装する必要があります。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 8 (d)	クラウドの採用が増加するにつれて、データ保護に使用される多くの暗号化キーの管理がより複雑になり、金融機関にとって新しい課題を生む場合があります。金融機関は、キーの生成、保管、配布を安全かつスケーラブルな方法で処理できる一元化されたキー管理システムの使用など、キー管理のために包括的で一元的な手法を採用する必要があります。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 8 (d)	クラウドの採用が増加するにつれて、データ保護に使用される多くの暗号化キーの管理がより複雑になり、金融機関にとって新しい課題を生む場合があります。金融機関は、キーの生成、保管、配布を安全かつスケーラブルな方法で処理できる一元化されたキー管理システムの使用など、キー管理のために包括的で一元的な手法を採用する必要があります。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 9 (a) ii)	管理プレーンは、従来のインフラストラクチャとデフォルトでリモートアクセスがサポートされているクラウドコンピューティングとのセキュリティ上の主な違いです。このアクセスレイヤーはサイバー攻撃を受けやすいため、全体的なクラウドデプロイの整合性が損なわれる可能性があります。このことから、金融機関は、次を含め、管理プレーンへのアクセスに対する強力な制御を確認する必要があります。ii)「最小特権」と強力な多要素認証 (MFA) を実装する。例えば、強力なパスワード、ソフトトークン、特権アクセス管理ツール、およびメーカーチェッカー機能。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 9 (a) ii)	管理プレーンは、従来のインフラストラクチャとデフォルトでリモートアクセスがサポートされているクラウドコンピューティングとのセキュリティ上の主な違いです。このアクセスレイヤーはサイバー攻撃を受けやすいため、全体的なクラウドデプロイの整合性が損なわれる可能性があります。このことから、金融機関は、次を含め、管理プレーンへのアクセスに対する強力な制御を確認する必要があります。ii)「最小特権」と強力な多要素認証 (MFA) を実装する。例えば、強力なパスワード、ソフトトークン、特権アクセス管理ツール、およびメーカーチェッカー機能。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 9 (a) ii)	管理プレーンは、従来のインフラストラクチャとデフォルトでリモートアクセスがサポートされているクラウドコンピューティングとのセキュリティ上の主な違いです。このアクセスレイヤーはサイバー攻撃を受けやすいため、全体的なクラウドデプロイの整合性が損なわれる可能性があります。このことから、金融機関は、次を含め、管理プレーンへのアクセスに対する強力な制御を確認する必要があります。ii)「最小特権」と強力な多要素認証 (MFA) を実装する。例えば、強力なパスワード、ソフトトークン、特権アクセス管理ツール、およびメーカーチェッカー機能。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 9 (a) ii)	管理プレーンは、従来のインフラストラクチャとデフォルトでリモートアクセスがサポートされているクラウドコンピューティングとのセキュリティ上の主な違いです。このアクセスレイヤーはサイバー攻撃を受けやすいため、全体的なクラウドデプロイの整合性が損なわれる可能性があります。このことから、金融機関は、次を含め、管理プレーンへのアクセスに対する強力な制御を確認する必要があります。ii)「最小特権」と強力な多要素認証 (MFA) を実装する。例えば、強力なパスワード、ソフトトークン、特権アクセス管理ツール、およびメーカーチェッカー機能。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 9 (a) iii)	管理プレーンは、従来のインフラストラクチャとデフォルトでリモートアクセスがサポートされているクラウドコンピューティングとのセキュリティ上の主な違いです。このアクセスレイヤーはサイバー攻撃を受けやすいため、全体的なクラウドデプロイの整合性が損なわれる可能性があります。このことから、金融機関は、次を含め、管理プレーンへのアクセスに対する強力な制御を確認する必要があります。iii) 特権のあるユーザーにはきめ細かい使用権限の割り当てを採用します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 9 (a) iii)	管理プレーンは、従来のインフラストラクチャとデフォルトでリモートアクセスがサポートされているクラウドコンピューティングとのセキュリティ上の主な違いです。このアクセスレイヤーはサイバー攻撃を受けやすいため、全体的なクラウドデプロイの整合性が損なわれる可能性があります。このことから、金融機関は、次を含め、管理プレーンへのアクセスに対する強力な制御を確認する必要があります。iii) 特権のあるユーザーにはきめ細かい使用権限の割り当てを採用します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 9 (a) iv)	管理プレーンは、従来のインフラストラクチャとデフォルトでリモートアクセスがサポートされているクラウドコンピューティングとのセキュリティ上の主な違いです。このアクセスレイヤーはサイバー攻撃を受けやすいため、全体的なクラウドデプロイの整合性が損なわれる可能性があります。このことから、金融機関は、次を含め、管理プレーンへのアクセスに対する強力な制御を確認する必要があります。iv) 特権のあるユーザーが実行するアクティビティへの継続的なモニタリングを実施すること。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 9 (a) iv)	管理プレーンは、従来のインフラストラクチャとデフォルトでリモートアクセスがサポートされているクラウドコンピューティングとのセキュリティ上の主な違いです。このアクセスレイヤーはサイバー攻撃を受けやすいため、全体的なクラウドデプロイの整合性が損なわれる可能性があります。このことから、金融機関は、次を含め、管理プレーンへのアクセスに対する強力な制御を確認する必要があります。iv) 特権のあるユーザーが実行するアクティビティへの継続的なモニタリングを実施すること。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 12 (a)	金融機関は、このポリシードキュメントの「データ損失防止」セクション (パラグラフ 11.14 ~ 11.16) で要求されているとおりに、クラウドサービスでホストされているデータを保護する必要があります。これには、金融機関がスタッフに自分のデバイスを使用して機密データにアクセスすることを許可した場合のエンドポイントフットプリントの拡大も含まれます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 12 (a)	金融機関は、このポリシードキュメントの「データ損失防止」セクション (パラグラフ 11.14 ~ 11.16) で要求されているとおりに、クラウドサービスでホストされているデータを保護する必要があります。これには、金融機関がスタッフに自分のデバイスを使用して機密データにアクセスすることを許可した場合のエンドポイントフットプリントの拡大も含まれます。	macie-status-check	Amazon Macie は、機械学習 (ML) とパターンマッチングを使用して、Amazon Simple Storage Service (Amazon S3) バケットに保存されている機密データを検出し、保護するのに役立つデータセキュリティサービスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 14 (c) i)	金融機関は、CIRP の開発において、次の追加措置を検討する必要があります。i) ダークウェブでのデータ漏えいを検知する機能を含め、効果的なインシデント管理を実現するために、セキュリティ違反インシデントを検出する能力を強化する。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
付録 10 パート B - 14 (c) i)	金融機関は、CIRP の開発において、次の追加措置を検討する必要があります。i) ダークウェブでのデータ漏えいを検知する機能を含め、効果的なインシデント管理を実現するために、セキュリティ違反インシデントを検出する能力を強化する。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for BNM RMiT」で入手できます。

カナダサイバーセキュリティセンター (CCCS) 中規模クラウド制御プロファイルに関する運用面のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレート

としてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下は、カナダサイバーセキュリティセンター (CCCS) の Medium Cloud Control Profile と AWS マネージド Config ルール間のマッピングの例です。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の CCCS Medium Cloud Control Profile コントロールに関連付けられます。CCCSC の中規模クラウド制御プロファイルは、複数の設定ルールと関連付けすることが可能です。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(1)	AC-2 (1) アカウント管理 | 自動システムのアカウント管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(3)	AC-2 (3) アカウント管理 | 非アクティブなアカウントの無効化	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(3)	AC-2 (3) アカウント管理 | 非アクティブなアカウントの無効化	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(4)	AC-2 (4) アカウント管理 | 自動監査アクション	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-AC-2(4)	AC-2 (4) アカウント管理 | 自動監査アクション	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(4)	AC-2 (4) アカウント管理 | 自動監査アクション	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(4)	AC-2 (4) アカウント管理 | 自動監査アクション	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(4)	AC-2 (4) アカウント管理 | 自動監査アクション	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(4)	AC-2 (4) アカウント管理 | 自動監査アクション	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2(4)	AC-2 (4) アカウント管理 | 自動監査アクション	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.A	AC-2.A アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.B	AC-2.B アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.C	AC-2.C アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.D	AC-2.D アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.E	AC-2.E アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.F	AC-2.F アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.G	AC-2.G アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.H	AC-2.H アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.I	AC-2.I アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.J	AC-2.J アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-2.K	AC-2.K アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-3.A	AC-3.A アクセスの適用	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4(21)	AC-4 (21) 情報フローの適用 | 情報フローの物理的/論理的分離	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-4(21)	AC-4 (21) 情報フローの適用 | 情報フローの物理的/論理的分離	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4(21)	AC-4 (21) 情報フローの適用 | 情報フローの物理的/論理的分離	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-4(21)	AC-4 (21) 情報フローの適用 | 情報フローの物理的/論理的分離	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4(21)	AC-4 (21) 情報フローの適用 | 情報フローの物理的/論理的分離	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-AC-4(21)	AC-4 (21) 情報フローの適用 | 情報フローの物理的/論理的分離	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-4(21)	AC-4 (21) 情報フローの適用 | 情報フローの物理的/論理的分離	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4(21)	AC-4 (21) 情報フローの適用 | 情報フローの物理的/論理的分離	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-4(21)	AC-4 (21) 情報フローの適用 | 情報フローの物理的/論理的分離	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-4.A	AC-4.A 情報フローの適用	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-5.A	AC-5.A 職務の分離	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-5.A	AC-5.A 職務の分離	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-5.A	AC-5.A 職務の分離	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-5.A	AC-5.A 職務の分離	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-5.A	AC-5.A 職務の分離	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(1)	AC-6 (1) 最小特権 | セキュリティ機能に対するアクセスの許可	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(1)	AC-6 (1) 最小特権 | セキュリティ機能に対するアクセスの許可	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(1)	AC-6 (1) 最小特権 | セキュリティ機能に対するアクセスの許可	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(1)	AC-6 (1) 最小特権 | セキュリティ機能に対するアクセスの許可	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(1)	AC-6 (1) 最小特権 | セキュリティ機能に対するアクセスの許可	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(2)	AC-6 (2) 最小特権 | 非セキュリティ機能に対する非特権アクセス	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(2)	AC-6 (2) 最小特権 | 非セキュリティ機能に対する非特権アクセス	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(2)	AC-6 (2) 最小特権 | 非セキュリティ機能に対する非特権アクセス	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(2)	AC-6 (2) 最小特権 | 非セキュリティ機能に対する非特権アクセス	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(2)	AC-6 (2) 最小特権 | 非セキュリティ機能に対する非特権アクセス	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(5)	AC-6 (5) 最小特権 | 特権アカウント	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(5)	AC-6 (5) 最小特権 | 特権アカウント	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(5)	AC-6 (5) 最小特権 | 特権アカウント	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(5)	AC-6 (5) 最小特権 | 特権アカウント	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
CCCS-fPBMM-AC-6(9)	AC-6 (9) 最小特権 | 特権を持つ機能の使用についての監査	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(9)	AC-6 (9) 最小特権 | 特権を持つ機能の使用についての監査	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-AC-6(9)	AC-6 (9) 最小特権 | 特権を持つ機能の使用についての監査	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(9)	AC-6 (9) 最小特権 | 特権を持つ機能の使用についての監査	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(9)	AC-6 (9) 最小特権 | 特権を持つ機能の使用についての監査	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(9)	AC-6 (9) 最小特権 | 特権を持つ機能の使用についての監査	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(9)	AC-6 (9) 最小特権 | 特権を持つ機能の使用についての監査	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(10)	AC-6 (10) 最小特権 | 非特権ユーザーによる特権関数の実行の禁止	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(10)	AC-6 (10) 最小特権 | 非特権ユーザーによる特権関数の実行の禁止	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(10)	AC-6 (10) 最小特権 | 非特権ユーザーによる特権関数の実行の禁止	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(10)	AC-6 (10) 最小特権 | 非特権ユーザーによる特権関数の実行の禁止	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6(10)	AC-6 (10) 最小特権 | 非特権ユーザーによる特権関数の実行の禁止	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-6.A	AC-6.A 最小特権	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(1)	AC-17 (1) リモートアクセス | 自動化されたモニタリングと制御	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(2)	AC-17 (2) リモートアクセス | 暗号化による機密性と整合性の保護	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-17(2)	AC-17 (2) リモートアクセス | 暗号化による機密性と整合性の保護	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(2)	AC-17 (2) リモートアクセス | 暗号化による機密性と整合性の保護	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(2)	AC-17 (2) リモートアクセス | 暗号化による機密性と整合性の保護	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-AC-17(2)	AC-17 (2) リモートアクセス | 暗号化による機密性と整合性の保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AC-17(2)	AC-17 (2) リモートアクセス | 暗号化による機密性と整合性の保護	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(3)	AC-17 (3) リモートアクセス | 管理型アクセスのコントロールポイント	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(4)	AC-17 (4) リモートアクセス | 特権を持つコマンドとアクセス	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(4)	AC-17 (4) リモートアクセス | 特権を持つコマンドとアクセス	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17(4)	AC-17 (4) リモートアクセス | 特権を持つコマンドとアクセス	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.A	AC-17.A リモートアクセス	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.AA	AC-17.AA リモートアクセス	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AC-17.B	AC-17.B リモートアクセス	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.A	AU-2.A 監査イベント	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.B	AU-2.B 監査イベント	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.C	AU-2.C 監査イベント	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-2.D	AU-2.D 監査イベント	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-AU-3(1)	AU-3 (1) 監査記録の内容 | 追加的な監査情報	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3(1)	AU-3 (1) 監査記録の内容 | 追加的な監査情報	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-AU-3(1)	AU-3 (1) 監査記録の内容 | 追加的な監査情報	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3(1)	AU-3 (1) 監査記録の内容 | 追加的な監査情報	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3(1)	AU-3 (1) 監査記録の内容 | 追加的な監査情報	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
CCCS-fPBMM-AU-3(1)	AU-3 (1) 監査記録の内容 | 追加的な監査情報	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3(1)	AU-3 (1) 監査記録の内容 | 追加的な監査情報	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3(1)	AU-3 (1) 監査記録の内容 | 追加的な監査情報	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	api-gw-execution-logging-enabled	API Gateway の口グ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-3.A	AU-3.A 監査記録の内容	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-5.A	AU-5.A 監査処理の失敗に対する対応	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-5.B	AU-5.B 監査処理の失敗に対する対応	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(1)	AU-6 (1) 監査のレビュー、分析、および報告 | プロセスの統合	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(1)	AU-6 (1) 監査のレビュー、分析、および報告 | プロセスの統合	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-AU-6(1)	AU-6 (1) 監査のレビュー、分析、および報告 | プロセスの統合	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(1)	AU-6 (1) 監査のレビュー、分析、および報告 | プロセスの統合	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(1)	AU-6 (1) 監査のレビュー、分析、および報告 | プロセスの統合	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(1)	AU-6 (1) 監査のレビュー、分析、および報告 | プロセスの統合	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	api-gw-execution-logging-enabled	API Gateway の口グ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-6(3)	AU-6 (3) 監査のレビュー、分析、および報告 | 監査リポジトリの相互関連付け	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-AU-7(1)	AU-7 (1) 監査の削減と報告の生成 | 自動処理	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-8.B	AU-8.B タイムスタンプ	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-9(2)	AU-9 (2) 監査情報の保護 | 分離された物理システムおよびコンポーネントによる監査内容のバックアップ	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-AU-9(2)	AU-9 (2) 監査情報の保護 | 分離された物理システムおよびコンポーネントによる監査内容のバックアップ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-9(2)	AU-9 (2) 監査情報の保護 | 分離された物理システムおよびコンポーネントによる監査内容のバックアップ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
CCCS-fPBMM-AU-9.A	AU-9.A 監査情報の保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-9.A	AU-9.A 監査情報の保護	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-9.A	AU-9.A 監査情報の保護	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
CCCS-fPBMM-AU-11.A	AU-11.A 監査記録の保持	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-11.B	AU-11.B 監査記録の保持	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
CCCS-fPBMM-AU-11.C	AU-11.C 監査記録の保持	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.A	AU-12.A 監査の生成	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-AU-12.C	AU-12.C 監査の生成	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-3(5)	CA-3 (5) システムの相互接続 | 外部ネットワークへの接続の制限	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	api-gw-xray-enabled	AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集し、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。X-Ray が を有効にして、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も表示できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.A	CA-7.A 継続的なモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	api-gw-xray-enabled	AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集し、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。X-Ray が を有効にして、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も表示できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.B	CA-7.B 継続的なモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	api-gw-xray-enabled	AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集し、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。X-Ray が を有効にして、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も表示できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.C	CA-7.C 継続的なモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	api-gw-xray-enabled	AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集し、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。X-Ray が を有効にして、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も表示できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.D	CA-7.D 継続的なモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	api-gw-xray-enabled	AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集し、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。X-Ray が を有効にして、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も表示できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.E	CA-7.E 継続的なモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	api-gw-xray-enabled	AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集し、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。X-Ray が を有効にして、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も表示できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.F	CA-7.F 継続的なモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	api-gw-xray-enabled	AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集し、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。X-Ray が を有効にして、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も表示できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-7.G	CA-7.G 継続的なモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CA-9.A	CA-9.A 内部システムの接続	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-2.A	CM-2.A ベースラインの設定	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-2.A	CM-2.A ベースラインの設定	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
CCCS-fPBMM-CM-2.A	CM-2.A ベースラインの設定	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-2.A	CM-2.A ベースラインの設定	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
CCCS-fPBMM-CM-2.A	CM-2.A ベースラインの設定	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-2.A	CM-2.A ベースラインの設定	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-2.A	CM-2.A ベースラインの設定	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.A	CM-3.A 設定変更の管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.A	CM-3.A 設定変更の管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.B	CM-3.B 設定変更の管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.B	CM-3.B 設定変更の管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.C	CM-3.C 設定変更の管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.C	CM-3.C 設定変更の管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.D	CM-3.D 設定変更の管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.D	CM-3.D 設定変更の管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.E	CM-3.E 設定変更の管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.E	CM-3.E 設定変更の管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.F	CM-3.F 設定変更の管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.F	CM-3.F 設定変更の管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.G	CM-3.G 設定変更の管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-3.G	CM-3.G 設定変更の管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(1)	CM-5 (1) 変更アクセスの制限 | 自動化されたアクセスの適用と監査	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5(5)	CM-5 (5) 変更アクセスの制限 | 本番向けおよび運用向け権限の制限	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-5.A	CM-5.A 変更アクセスの制限	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6(1)	CM-6 (1) 構成の設定 | 自動化された一元管理、アプリケーション、および検証	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6(1)	CM-6 (1) 構成の設定 | 自動化された一元管理、アプリケーション、および検証	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6(1)	CM-6 (1) 構成の設定 | 自動化された一元管理、アプリケーション、および検証	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.A	CM-6.A 構成の設定	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.B	CM-6.B 構成の設定	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.C	CM-6.C 構成の設定	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-6.D	CM-6.D 構成の設定	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-7.A	CM-7.A 最小限の機能	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-7.A	CM-7.A 最小限の機能	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-7.B	CM-7.B 最小限の機能	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-7.B	CM-7.B 最小限の機能	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8(1)	CM-8 (1) 情報システムコンポーネントのインベントリ | インストール中あるいは削除中の更新	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8(1)	CM-8 (1) 情報システムコンポーネントのインベントリ | インストール中あるいは削除中の更新	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8(2)	CM-8 (2) 情報システムコンポーネントのインベントリ | 自動化されたメンテナンス	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8(2)	CM-8 (2) 情報システムコンポーネントのインベントリ | 自動化されたメンテナンス	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8(3)	CM-8 (3) 情報システムコンポーネントのインベントリ | 非認証コンポーネントの自動検出	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8(3)	CM-8 (3) 情報システムコンポーネントのインベントリ | 非認証コンポーネントの自動検出	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8(3)	CM-8 (3) 情報システムコンポーネントのインベントリ | 非認証コンポーネントの自動検出	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-CM-8(3)	CM-8 (3) 情報システムコンポーネントのインベントリ | 非認証コンポーネントの自動検出	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.A	CM-8.A 情報システムコンポーネントのインベントリ	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.A	CM-8.A 情報システムコンポーネントのインベントリ	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.B	CM-8.B 情報システムのコンポーネントのインベントリ	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.B	CM-8.B 情報システムのコンポーネントのインベントリ	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.C	CM-8.C 情報システムのコンポーネントのインベントリ	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.C	CM-8.C 情報システムのコンポーネントのインベントリ	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.D	CM-8.D 情報システムのコンポーネントのインベントリ	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.D	CM-8.D 情報システムのコンポーネントのインベントリ	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.E	CM-8.E 情報システムのコンポーネントのインベントリ	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CM-8.E	CM-8.E 情報システムのコンポーネントのインベントリ	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(5)	CP-2 (5) 緊急時対応計画 | 重要なミッションとビジネス機能の継続	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(6)	CP-2 (6) 緊急時対応計画 | 代替的なプロセス処理とストレージサイト	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(6)	CP-2 (6) 緊急時対応計画 | 代替的なプロセス処理とストレージサイト	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(6)	CP-2 (6) 緊急時対応計画 | 代替的なプロセス処理とストレージサイト	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(6)	CP-2 (6) 緊急時対応計画 | 代替的なプロセス処理とストレージサイト	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2(6)	CP-2 (6) 緊急時対応計画 | 代替的なプロセス処理とストレージサイト	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-2(6)	CP-2 (6) 緊急時対応計画 | 代替的なプロセス処理とストレージサイト	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.A	CP-2.A 緊急時対応計画	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.A	CP-2.A 緊急時対応計画	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
CCCS-fPBMM-CP-2.A	CP-2.A 緊急時対応計画	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.A	CP-2.A 緊急時対応計画	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.A	CP-2.A 緊急時対応計画	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.A	CP-2.A 緊急時対応計画	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.A	CP-2.A 緊急時対応計画	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-2.A	CP-2.A 緊急時対応計画	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.B	CP-2.B 緊急時対応計画	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.B	CP-2.B 緊急時対応計画	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
CCCS-fPBMM-CP-2.B	CP-2.B 緊急時対応計画	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.B	CP-2.B 緊急時対応計画	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.B	CP-2.B 緊急時対応計画	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.B	CP-2.B 緊急時対応計画	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.B	CP-2.B 緊急時対応計画	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-2.B	CP-2.B 緊急時対応計画	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.C	CP-2.C 緊急時対応計画	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.C	CP-2.C 緊急時対応計画	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
CCCS-fPBMM-CP-2.C	CP-2.C 緊急時対応計画	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.C	CP-2.C 緊急時対応計画	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.C	CP-2.C 緊急時対応計画	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.C	CP-2.C 緊急時対応計画	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.C	CP-2.C 緊急時対応計画	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-2.C	CP-2.C 緊急時対応計画	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.D	CP-2.D 緊急時対応計画	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.D	CP-2.D 緊急時対応計画	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
CCCS-fPBMM-CP-2.D	CP-2.D 緊急時対応計画	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.D	CP-2.D 緊急時対応計画	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.D	CP-2.D 緊急時対応計画	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.D	CP-2.D 緊急時対応計画	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.D	CP-2.D 緊急時対応計画	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-2.D	CP-2.D 緊急時対応計画	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.E	CP-2.E 緊急時対応計画	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.E	CP-2.E 緊急時対応計画	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
CCCS-fPBMM-CP-2.E	CP-2.E 緊急時対応計画	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.E	CP-2.E 緊急時対応計画	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.E	CP-2.E 緊急時対応計画	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.E	CP-2.E 緊急時対応計画	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.E	CP-2.E 緊急時対応計画	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-2.E	CP-2.E 緊急時対応計画	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.F	CP-2.F 緊急時対応計画	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.F	CP-2.F 緊急時対応計画	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
CCCS-fPBMM-CP-2.F	CP-2.F 緊急時対応計画	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.F	CP-2.F 緊急時対応計画	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.F	CP-2.F 緊急時対応計画	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.F	CP-2.F 緊急時対応計画	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.F	CP-2.F 緊急時対応計画	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-2.F	CP-2.F 緊急時対応計画	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.G	CP-2.G 緊急時対応計画	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.G	CP-2.G 緊急時対応計画	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
CCCS-fPBMM-CP-2.G	CP-2.G 緊急時対応計画	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.G	CP-2.G 緊急時対応計画	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.G	CP-2.G 緊急時対応計画	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.G	CP-2.G 緊急時対応計画	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-2.G	CP-2.G 緊急時対応計画	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-2.G	CP-2.G 緊急時対応計画	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(1)	CP-6 (1) 代替のストレージサイト | プライマリサイトからの分離	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6(2)	CP-6 (2) 代替のストレージサイト | 目標復旧時間と目標復旧ポイント	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認しますAWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.A	CP-6.A 代替のストレージサイト	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	バックアップ計画によって保護されたEBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-6.B	CP-6.B 代替のストレージサイト	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(3)	CP-9 (3) 情報システムのバックアップ | 重要な情報のための分離されたストレージ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(7)	CP-9 (7) 情報システムのバックアップ | 二重認可	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9(7)	CP-9 (7) 情報システムのバックアップ | 二重認可	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	バックアップ計画によって保護されたEBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.A	CP-9.A 情報システムのバックアップ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.AA	CP-9.AA 情報システムのバックアップ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	バックアップ計画によって保護されたEBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.B	CP-9.B 情報システムのバックアップ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	バックアップ計画によって保護されたEBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.C	CP-9.C 情報システムのバックアップ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	バックアップ計画によって保護されたEBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-9.D	CP-9.D 情報システムのバックアップ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-CP-10.A	CP-10.A 情報システムの復旧と再構築	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(1)	IA-2 (1) 身分証明書と認証 (組織のユーザー) | 特権アカウントへのネットワークアクセス	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(1)	IA-2 (1) 身分証明書と認証 (組織のユーザー) | 特権アカウントへのネットワークアクセス	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(1)	IA-2 (1) 身分証明書と認証 (組織のユーザー) | 特権アカウントへのネットワークアクセス	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(3)	IA-2 (3) 身分証明書と認証 (組織のユーザー) | 特権アカウントへのローカルアクセス	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(3)	IA-2 (3) 身分証明書と認証 (組織のユーザー) | 特権アカウントへのローカルアクセス	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(3)	IA-2 (3) 身分証明書と認証 (組織のユーザー) | 特権アカウントへのローカルアクセス	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(8)	IA-2 (8) 身分証明書と認証 (組織のユーザー) | 特権アカウントへのネットワークアクセス – リプレイへの耐性	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(8)	IA-2 (8) 身分証明書と認証 (組織のユーザー) | 特権アカウントへのネットワークアクセス – リプレイへの耐性	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(8)	IA-2 (8) 身分証明書と認証 (組織のユーザー) | 特権アカウントへのネットワークアクセス – リプレイへの耐性	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(11)	IA-2 (11) 身分証明書と認証 (組織のユーザー) | リモートアクセス – 個別のデバイス	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(11)	IA-2 (11) 身分証明書と認証 (組織のユーザー) | リモートアクセス – 個別のデバイス	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2(11)	IA-2 (11) 身分証明書と認証 (組織のユーザー) | リモートアクセス – 個別のデバイス	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2.A	IA-2.A 身分証明書と認証 (組織のユーザー)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-2.A	IA-2.A 身分証明書と認証 (組織のユーザー)	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2.A	IA-2.A 身分証明書と認証 (組織のユーザー)	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-2.A	IA-2.A 身分証明書と認証 (組織のユーザー)	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4(4)	IA-4 (4) 識別子の管理 | ユーザーステータスの識別	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.A	IA-4.A 識別子の管理	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.A	IA-4.A 識別子の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-4.A	IA-4.A 識別子の管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.B	IA-4.B 識別子の管理	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.B	IA-4.B 識別子の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-4.B	IA-4.B 識別子の管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.C	IA-4.C 識別子の管理	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.C	IA-4.C 識別子の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-4.C	IA-4.C 識別子の管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.D	IA-4.D 識別子の管理	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.D	IA-4.D 識別子の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-4.D	IA-4.D 識別子の管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.E	IA-4.E 識別子の管理	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-4.E	IA-4.E 識別子の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-4.E	IA-4.E 識別子の管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5(1)	IA-5 (1) Authenticator の管理 | パスワードベースの認証	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5(2)	IA-5 (2) Authenticator の管理 | PKI ベースの認証	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5(2)	IA-5 (2) Authenticator の管理 | PKI ベースの認証	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5(4)	IA-5 (4) Authenticator の管理 | 自動的なパスワード強度特定のサポート	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5(8)	IA-5 (8) Authenticator の管理 | 複数の情報システムのアカウント	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5(8)	IA-5 (8) Authenticator の管理 | 複数の情報システムのアカウント	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5(8)	IA-5 (8) Authenticator の管理 | 複数の情報システムのアカウント	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.A	IA-5.A Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.A	IA-5.A Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.A	IA-5.A Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.A	IA-5.A Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.B	IA-5.B Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.B	IA-5.B Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.B	IA-5.B Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.B	IA-5.B Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.C	IA-5.C Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.C	IA-5.C Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.C	IA-5.C Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.C	IA-5.C Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.D	IA-5.D Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.D	IA-5.D Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.D	IA-5.D Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.D	IA-5.D Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.E	IA-5.E Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.E	IA-5.E Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.E	IA-5.E Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.E	IA-5.E Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.F	IA-5.F Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.F	IA-5.F Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.F	IA-5.F Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.F	IA-5.F Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.G	IA-5.G Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.G	IA-5.G Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.G	IA-5.G Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.G	IA-5.G Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.H	IA-5.H Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.H	IA-5.H Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.H	IA-5.H Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.H	IA-5.H Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.I	IA-5.I Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.I	IA-5.I Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.I	IA-5.I Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.I	IA-5.I Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.J	IA-5.J Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
CCCS-fPBMM-IA-5.J	IA-5.J Authenticator の管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.J	IA-5.J Authenticator の管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IA-5.J	IA-5.J Authenticator の管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-IR-6(1)	IR-6 (1) インシデントの報告 | 自動化された報告	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-3.A	MA-3.A メンテナンスツール	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-3.A	MA-3.A メンテナンスツール	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MA-4(1)	MA-4 (1) 非ローカルでのメンテナンス | 監査とレビュー	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-MP-2.A	MP-2.A メディアへのアクセス	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-RA-5.A	RA-5.A 脆弱性スキャン	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-RA-5.B	RA-5.B 脆弱性スキャン	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-RA-5.C	RA-5.C 脆弱性スキャン	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-RA-5.D	RA-5.D 脆弱性スキャン	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-RA-5.E	RA-5.E 脆弱性スキャン	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SA-10(1)	SA-10 (1) デベロッパー向け設定の管理 | ソフトウェアおよびファームウェアの整合性の検証	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-5.A	SC-5.A サービス拒否からの保護	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-5.A	SC-5.A サービス拒否からの保護	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-6.A	SC-6.A リソースの可用性	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-6.A	SC-6.A リソースの可用性	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-6.A	SC-6.A リソースの可用性	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-6.A	SC-6.A リソースの可用性	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-SC-6.A	SC-6.A リソースの可用性	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-6.A	SC-6.A リソースの可用性	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-6.A	SC-6.A リソースの可用性	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CCCS-fPBMM-SC-6.A	SC-6.A リソースの可用性	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(3)	SC-7 (3) 境界の保護 | アクセスポイント	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(4)	SC-7 (4) 境界の保護 | 外部のテレコミュニケーションサービス	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(5)	SC-7 (5) 境界の保護 | デフォルトによる拒否と例外による許可	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(5)	SC-7 (5) 境界の保護 | デフォルトによる拒否と例外による許可	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(5)	SC-7 (5) 境界の保護 | デフォルトによる拒否と例外による許可	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(5)	SC-7 (5) 境界の保護 | デフォルトによる拒否と例外による許可	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7(7)	SC-7 (7) 境界の保護 | リモートデバイスに対するスプリットトンネリングの防止	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.A	SC-7.A 境界の保護	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.B	SC-7.B 境界の保護	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-7.C	SC-7.C 境界の保護	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-8(1)	SC-8 (1) 伝送の機密性と整合性 | 暗号化または代替の物理的保護	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-8(1)	SC-8 (1) 伝送の機密性と整合性 | 暗号化または代替の物理的保護	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-8(1)	SC-8 (1) 伝送の機密性と整合性 | 暗号化または代替の物理的保護	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-8(1)	SC-8 (1) 伝送の機密性と整合性 | 暗号化または代替の物理的保護	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-8(1)	SC-8 (1) 伝送の機密性と整合性 | 暗号化または代替の物理的保護	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-SC-8(1)	SC-8 (1) 伝送の機密性と整合性 | 暗号化または代替の物理的保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-8(1)	SC-8 (1) 伝送の機密性と整合性 | 暗号化または代替の物理的保護	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-8(1)	SC-8 (1) 伝送の機密性と整合性 | 暗号化または代替の物理的保護	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-8(1)	SC-8 (1) 伝送の機密性と整合性 | 暗号化または代替の物理的保護	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-8.A	SC-8.A 伝送の機密性と整合性	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-8.A	SC-8.A 伝送の機密性と整合性	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-8.A	SC-8.A 伝送の機密性と整合性	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-8.A	SC-8.A 伝送の機密性と整合性	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-8.A	SC-8.A 伝送の機密性と整合性	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-SC-8.A	SC-8.A 伝送の機密性と整合性	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-8.A	SC-8.A 伝送の機密性と整合性	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-8.A	SC-8.A 伝送の機密性と整合性	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-8.A	SC-8.A 伝送の機密性と整合性	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-12(1)	SC-12 (1) 暗号化キーの確立と管理 | 可用性	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
CCCS-fPBMM-SC-12(2)	SC-12 (2) 暗号化キーの確立と管理 | 対象キー	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-12(2)	SC-12 (2) 暗号化キーの確立と管理 | 対象キー	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
CCCS-fPBMM-SC-12.A	SC-12.A 暗号化キーの確立と管理	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-12.A	SC-12.A 暗号化キーの確立と管理	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-13.A	SC-13.A 暗号化による保護	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-22.A	SC-22.A 名前およびアドレスの解決サービス用のアーキテクチャとプロビジョニング	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
CCCS-fPBMM-SC-23.A	SC-23.A セッションの認証性	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-23.A	SC-23.A セッションの認証性	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
CCCS-fPBMM-SC-23.A	SC-23.A セッションの認証性	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-23.A	SC-23.A セッションの認証性	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-23.A	SC-23.A セッションの認証性	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-SC-23.A	SC-23.A セッションの認証性	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-23.A	SC-23.A セッションの認証性	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-23.A	SC-23.A セッションの認証性	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-23.A	SC-23.A セッションの認証性	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28(1)	SC-28 (1) 保存中の情報に対する保護 | 暗号化による保護	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CCCS-fPBMM-SC-28.A	SC-28.A 保存中の情報に対する保護	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(2)	SI-2 (2) 欠陥修復 | 自動的な欠陥修復のステータス	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2(3)	SI-2 (3) 欠陥の修復 | 欠陥の修復にかかる時間/修正アクションに関するベンチマーク	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.A	SI-2.A 欠陥修復	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.B	SI-2.B 欠陥修復	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.C	SI-2.C 欠陥修復	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-2.D	SI-2.D 欠陥修復	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3(1)	SI-3 (1) 悪意のあるコードからの保護 | 一元的な管理	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3(7)	SI-3 (7) 悪意のあるコードからの保護 | 署名ベース以外での検出	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.A	SI-3.A 悪意のあるコードからの保護	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.A	SI-3.A 悪意のあるコードからの保護	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.A	SI-3.A 悪意のあるコードからの保護	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.A	SI-3.A 悪意のあるコードからの保護	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-SI-3.A	SI-3.A 悪意のあるコードからの保護	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.B	SI-3.B 悪意のあるコードからの保護	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.B	SI-3.B 悪意のあるコードからの保護	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.B	SI-3.B 悪意のあるコードからの保護	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-SI-3.B	SI-3.B 悪意のあるコードからの保護	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.C	SI-3.C 悪意のあるコードからの保護	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.C	SI-3.C 悪意のあるコードからの保護	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.C	SI-3.C 悪意のあるコードからの保護	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-SI-3.C	SI-3.C 悪意のあるコードからの保護	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.D	SI-3.D 悪意のあるコードからの保護	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.D	SI-3.D 悪意のあるコードからの保護	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-3.D	SI-3.D 悪意のあるコードからの保護	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CCCS-fPBMM-SI-3.D	SI-3.D 悪意のあるコードからの保護	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(1)	SI-4 (1) 情報システムのモニタリング | システム全体の侵入検知システム	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(1)	SI-4 (1) 情報システムのモニタリング | システム全体の侵入検知システム	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(2)	SI-4 (2) 情報システムのモニタリング | リアルタイム分析のための自動化ツール	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(2)	SI-4 (2) 情報システムのモニタリング | リアルタイム分析のための自動化ツール	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(4)	SI-4 (4) 情報システムのモニタリング | インバウンドとアウトバウンドの通信トラフィック	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(4)	SI-4 (4) 情報システムのモニタリング | インバウンドとアウトバウンドの通信トラフィック	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(5)	SI-4 (5) 情報システムのモニタリング | システムで生成されたアラート	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(11)	SI-4 (11) 情報システムのモニタリング | 通信トラフィックにおける異常の分析	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(11)	SI-4 (11) 情報システムのモニタリング | 通信トラフィックにおける異常の分析	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(16)	SI-4 (16) 情報システムのモニタリング | モニタリング情報の相互関連付け	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(16)	SI-4 (16) 情報システムのモニタリング | モニタリング情報の相互関連付け	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(20)	SI-4 (20) 情報システムのモニタリング | 特権ユーザー	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(23)	SI-4 (23) 情報システムのモニタリング | ホストベースのデバイス	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4(23)	SI-4 (23) 情報システムのモニタリング | ホストベースのデバイス	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.A	SI-4.A 情報システムのモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.A	SI-4.A 情報システムのモニタリング	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.A	SI-4.A 情報システムのモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CCCS-fPBMM-SI-4.A	SI-4.A 情報システムのモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.A	SI-4.A 情報システムのモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.B	SI-4.B 情報システムのモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.B	SI-4.B 情報システムのモニタリング	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.B	SI-4.B 情報システムのモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CCCS-fPBMM-SI-4.B	SI-4.B 情報システムのモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.B	SI-4.B 情報システムのモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.C	SI-4.C 情報システムのモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.C	SI-4.C 情報システムのモニタリング	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.C	SI-4.C 情報システムのモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CCCS-fPBMM-SI-4.C	SI-4.C 情報システムのモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.C	SI-4.C 情報システムのモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.D	SI-4.D 情報システムのモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.D	SI-4.D 情報システムのモニタリング	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.D	SI-4.D 情報システムのモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CCCS-fPBMM-SI-4.D	SI-4.D 情報システムのモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.D	SI-4.D 情報システムのモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.E	SI-4.E 情報システムのモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.E	SI-4.E 情報システムのモニタリング	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.E	SI-4.E 情報システムのモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CCCS-fPBMM-SI-4.E	SI-4.E 情報システムのモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.E	SI-4.E 情報システムのモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.F	SI-4.F 情報システムのモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.F	SI-4.F 情報システムのモニタリング	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.F	SI-4.F 情報システムのモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CCCS-fPBMM-SI-4.F	SI-4.F 情報システムのモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.F	SI-4.F 情報システムのモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.G	SI-4.G 情報システムのモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.G	SI-4.G 情報システムのモニタリング	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.G	SI-4.G 情報システムのモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CCCS-fPBMM-SI-4.G	SI-4.G 情報システムのモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-4.G	SI-4.G 情報システムのモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-5.A	SI-5.A セキュリティアラート、勧告、および指示	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-5.B	SI-5.B セキュリティアラート、勧告、および指示	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-5.C	SI-5.C セキュリティアラート、勧告、および指示	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-5.D	SI-5.D セキュリティアラート、勧告、および指示	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-7(1)	SI-7 (1) ソフトウェア、ファームウェア、および情報の整合性 | 整合性の確認	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-7(7)	SI-7 (7) ソフトウェア、ファームウェア、および情報の整合性 | 検出と対応の統合	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-7.A	SI-7.A ソフトウェア、ファームウェア、および情報の整合性	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CCCS-fPBMM-SI-12.A	SI-12.A 情報の取り扱いと保持	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile」(カナダサイバーセキュリティセンター (CCCS) 中規模クラウド制御プロファイルに関する運用面のベストプラクティス) で入手できます。

CIS AWS Foundations Benchmark v1.4 Level 1 に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 1 と AWS マネージド Config ルール/AWS Config プロセスチェック間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の CIS Amazon Web Services Foundation v1.4 Level 1 コントロールに関連付けられます。CIS の「Amazon Web Services Foundation v1.4 Level

1」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

プロセスチェックの詳細については、「process-checks」を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	現在の連絡先情報を維持します	account-contact-details-configured (Process Check)	AWS アカウントの連絡先の E メールと電話番号が最新のものであり、組織内の 1 人以上の個人にマッピングされていることを確認します。コンソールの [My Account] (マイアカウント) セクションで、[Contact Information] (連絡先情報) セクションに正しい情報が指定されていることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2	セキュリティの連絡先情報が登録されていることを確認します。	account-security-contact-configured (Process Check)	組織のセキュリティチームの連絡先の E メールと電話番号が最新のものであることを確認します。 AWS マネジメントコンソールのマイアカウントセクションで、セキュリティセクションに正しい情報が指定されていることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4	「ルート」ユーザーのアクセスキーが存在しないことを確認する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5	MFA が「ルート」ユーザーで有効になっていることを確認する	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.7	管理および日常のタスクでの「root」ユーザーの使用を排除します	root-account-regular-use (Process Check)	日常的なタスクで、ルートアカウントを使用しないようにしてください。IAM で認証情報レポートを実行し、ルートユーザーが最後に使用された時期を調べます。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.8	IAM パスワードポリシーにおいて 14 文字以上の長さが必要になります。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.9	IAM パスワードポリシーはパスワードの再使用を禁止しています	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.10	コンソールパスワードを持っているすべてのユーザーについて多要素認証 (MFA) が有効であることを確認します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.11	コンソールパスワードを持つすべてのユーザーの初期ユーザー集合アップ中にアクセスキーを集合アップしないでください	iam-user-console-and-api-access-at-creation (Process Check)	コンソールのパスワードを持つすべてのユーザーの初期設定時に、アクセスキーが設定されないようにします。コンソールにアクセスできるすべてのユーザーについて、ユーザーの「作成時刻」とアクセスキーの「作成日」を比較します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.12	45 日間以上使用されていない認証情報は無効にします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge の値を設定する必要があります (CIS スタンダード値デフォルト: 45)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.13	1 人のユーザーが使用できるアクティブなアクセスキーが 1 つのみであることを確認します。	iam-user-single-access-key (Process Check)	1 人のユーザーが使用できるアクティブなアクセスキーが 1 つのみであることを確認します。すべてのユーザーについて、[Security Credentials] (認証情報) タブで IAM の各ユーザーに使用されているアクティブなキーが 1 つのみであることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.14	アクセスキーは 90 日ごとに更新します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.15	ユーザーがグループを通してのみアクセス権を受け取るようにします。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.15	ユーザーがグループを通してのみアクセス権を受け取るようにします。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.15	ユーザーがグループを通してのみアクセス権を受け取るようにします。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.16	完全な「*:*」管理権限を許可する IAM ポリシーは作成されません。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.17	サポートでインシデントを管理するための AWS サポートロールが作成されていることを確認します。	iam-policy-in-use	AWS Identity and Access Management (IAM) は、IAM ポリシーが適切なユーザー、ロール、またはグループに割り当てられるようにすることで、アクセス許可と認可を管理するのに役立ちます。これらのポリシーを制限することは、最小特権と職務分離の原則も組み込まれています。このルールでは、 AWS Support でのインシデント管理のために、policyARN を arn:aws:iam::aws:policy/AWSSupportAccess に設定することが要求されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.19	AWS IAM に保存されている期限切れの SSL/TLS 証明書が、すべて削除されていることを確認します。	iam-expired-certificates (Process Check)	IAM に保存されている期限切れの SSL/TLS 証明書が、すべて削除されていることを確認します。CLI AWS がインストールされているコマンドラインから AWS 「iam list-server-certificates」コマンドを実行し、期限切れのサーバー証明書があるかどうかを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.20	IAM Access Analyzer AWS が有効になっていることを確認する	iam-access-analyzer-enabled (Process Check)	IAM Access Analyzer が有効になっていることを確認します。コンソールの [IAM] セクションで、[Access Analyzer] (アクセスアナライザー) を選択し、[STATUS] が [Active] (有効) に設定されていることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1.3	S3 バケットで MFA Delete が有効であることを確認する。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。S3 バケットに多要素認証 (MFA) 削除を追加すると、バケットのバージョン状態を変更したり、オブジェクトのバージョンを削除したりするために、追加の認証要素が必要になります。MFA 削除により、万が一、セキュリティ認証が漏洩したり、不正なアクセスが行われた場合でも、セキュリティのレイヤーを追加することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1.5	S3バケットに「パブリックアクセスをブロックする (バケット設定) 」が設定されていることを確認する	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1.5	S3バケットに「パブリックアクセスをブロックする (バケット設定) 」が設定されていることを確認する	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
2.2.1	EBSボリュームの暗号化が有効であることを確認します	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.1	EBSボリュームの暗号化が有効であることを確認します	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2.3.1	RDSインスタンスで暗号化が有効であることを確認します	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.3.1	RDSインスタンスで暗号化が有効であることを確認します	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1	CloudTrail はすべてのリージョンで有効になっていることを確認します	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	CloudTrail ログの保存に使用されるS3 バケットが一般公開されていないことを確認します	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.3	CloudTrail ログの保存に使用されるS3 バケットが一般公開されていないことを確認します	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	CloudTrail ログの保存に使用されるS3 バケットが一般公開されていないことを確認します	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
3.4	CloudTrailトレイルが CloudWatchLogs と統合されていることを確認します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6	S3 バケットアクセスログ記録が CloudTrail S3 バケットで有効になっていることを確認します	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します	alarm-unauthorized-api-calls (Process Check)	不正な API コールに対するログメトリクスフィルターとアラームが存在することを確認します このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2	MFA を使用しないマネジメントコンソールサインインに対してログメトリクスフィルターとアラームが存在することを確認します	alarm-sign-in-without-mfa (Process Check)	多要素認証 (MFA) を使用しない AWS マネジメントコンソールのサインインに対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.3	「ルート」アカウントに対してログメトリクスフィルターとアラームが存在することを確認します	alarm-root-account-use (Process Check)	ルートアカウントに対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4	MFA なしの IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認します。	alarm-iam-policy-change (Process Check)	IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.5	CloudTrail の設定の変更に対するログメトリクスフィルターとアラームが存在することを確認します。	alarm-cloudtrail-config-change (Process Check)	AWS CloudTrail 設定の変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8	S3 バケットの変更に対してログメトリクスフィルターとアラームが存在することを確認します	alarm-s3-bucket-policy-change (Process Check)	Amazon S3 バケットのポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.12	ネットワークゲートウェイへの変更に対するログメトリクスとアラームが存在することを確認します	alarm-vpc-network-gateway-change (Process Check)	ネットワークゲートウェイへの変更に対するログメトリクスとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.13	ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します	alarm-vpc-route-table-change (Process Check)	ルートテーブルの変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.14	VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します	alarm-vpc-change (Process Check)	Amazon Virtual Private Cloud (Amazon VPC) の変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.15	AWS Organizations の変更に対するログメトリクスフィルターとアラームが存在することを確認する	alarm-organizations-change (Process Check)	AWS Organizations の変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.1	ネットワーク ACL が 0.0.0.0/0 からリモートサーバー管理ポートへの侵入を許可していないことを確認します	nacl-no-unrestricted-ssh-rdp	ネットワーク ACL で、リモートサーバーの管理ポートへのパブリック Ingress が許可されていないことを確認します。コンソールの [VPC] セクションで、ソースが「0.0.0.0/0」のネットワーク ACL があり、リモートサーバーの管理者ポートを含むポートまたはポート範囲が許可されていることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	ネットワーク ACL が 0.0.0.0/0 からリモートサーバー管理ポートへの侵入を許可していないことを確認します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	ネットワーク ACL が 0.0.0.0/0 からリモートサーバー管理ポートへの侵入を許可していないことを確認します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 ~ blockedPort5 パラメータ (CIS標準値: 3389) を任意に設定することができます。実際の値には、組織のポリシーを反映する必要があります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1」で入手できます。

CIS AWS Foundations Benchmark v1.4 Level 2 の運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 2 と AWS マネージド Config ルール/AWS Config プロセスチェック間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の CIS Amazon Web Services Foundation v1.4 Level 2 コントロールに関連付けられます。CIS の「Amazon Web Services Foundation v1.4 Level 2」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

プロセスチェックの詳細については、「process-checks」を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	現在の連絡先情報を維持します	account-contact-details-configured (Process Check)	AWS アカウントの連絡先の E メールと電話番号が最新のものであり、組織内の 1 人以上の個人にマッピングされていることを確認します。コンソールの [My Account] (マイアカウント) セクションで、[Contact Information] (連絡先情報) セクションに正しい情報が指定されていることを確認します。このコント

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2	セキュリティの連絡先情報が登録されていることを確認します。	account-security-contact-configured (Process Check)	組織のセキュリティチームの連絡先の E メールと電話番号が最新のものであることを確認します。 AWS マネジメントコンソールのマイアカウントセクションで、セキュリティセクションに正しい情報が指定されていることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4	「ルート」ユーザーのアクセスキーが存在しないことを確認する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5	MFA が「ルート」ユーザーで有効になっていることを確認する	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.6	「ルート」ユーザーアカウントでハードウェア MFA を有効にします	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.7	管理および日常のタスクでの「root」ユーザーの使用を排除します	root-account-regular-use (Process Check)	日常的なタスクで、ルートアカウントを使用しないようにしてください。IAM で認証情報レポートを実行し、ルートユーザーが最後に使用された時期を調べます。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.8	IAM パスワードポリシーにおいて 14 文字以上の長さが必要になります。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.9	IAM パスワードポリシーはパスワードの再使用を禁止しています	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.10	コンソールパスワードを持っているすべてのユーザーについて多要素認証 (MFA) が有効であることを確認します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.11	コンソールパスワードを持つすべてのユーザーの初期ユーザー集合アップ中にアクセスキーを集合アップしないでください	iam-user-console-and-api-access-at-creation (Process Check)	コンソールのパスワードを持つすべてのユーザーの初期設定時に、アクセスキーが設定されないようにします。コンソールにアクセスできるすべてのユーザーについて、ユーザーの「作成時刻」とアクセスキーの「作成日」を比較します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.12	45 日間以上使用されていない認証情報は無効にします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge の値を設定する必要があります (CIS スタンダード値デフォルト: 45)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.13	1 人のユーザーが使用できるアクティブなアクセスキーが 1 つのみであることを確認します。	iam-user-single-access-key (Process Check)	1 人のユーザーが使用できるアクティブなアクセスキーが 1 つのみであることを確認します。すべてのユーザーについて、[Security Credentials] (認証情報) タブで IAM の各ユーザーに使用されているアクティブなキーが 1 つのみであることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.14	アクセスキーは 90 日ごとに更新します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.15	ユーザーがグループを通してのみアクセス権を受け取るようにします。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.15	ユーザーがグループを通してのみアクセス権を受け取るようにします。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.15	ユーザーがグループを通してのみアクセス権を受け取るようにします。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.16	完全な「*:*」管理権限を許可する IAM ポリシーは作成されません。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.17	サポートでインシデントを管理するための AWS サポートロールが作成されていることを確認します。	iam-policy-in-use	AWS Identity and Access Management (IAM) は、IAM ポリシーが適切なユーザー、ロール、またはグループに割り当てられるようにすることで、アクセス許可と認可を管理するのに役立ちます。これらのポリシーを制限することは、最小特権と職務分離の原則も組み込まれています。このルールでは、 AWS Support でのインシデント管理のために、policyARN を arn:aws:iam::aws:policy/AWSSupportAccess に設定することが要求されます。
1.18	インスタンスからの AWS リソースアクセスに IAM インスタンスロールが使用されていることを確認する	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.19	AWS IAM に保存されている期限切れの SSL/TLS 証明書が、すべて削除されていることを確認します。	iam-expired-certificates (Process Check)	IAM に保存されている期限切れの SSL/TLS 証明書が、すべて削除されていることを確認します。CLI AWS がインストールされているコマンドラインから AWS 「iam list-server-certificates」コマンドを実行し、期限切れのサーバー証明書があるかどうかを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.20	IAM Access Analyzer AWS が有効になっていることを確認する	iam-access-analyzer-enabled (Process Check)	IAM Access Analyzer が有効になっていることを確認します。コンソールの [IAM] セクションで、[Access Analyzer] (アクセスアナライザー) を選択し、[STATUS] が [Active] (有効) に設定されていることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.21	マルチアカウント環境の ID フェデレーションまたは AWS Organizations からユーザーが一元管理されていることを確認します。	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
2.1.1	すべての S3 バケットが encryption-at-rest を採用していることを確認します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1.2	S3 Bucket Policy が HTTP リクエストを拒否するように設定されていることを確認します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1.3	S3 バケットで MFA Delete が有効であることを確認する。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。S3 バケットに多要素認証 (MFA) 削除を追加すると、バケットのバージョン状態を変更したり、オブジェクトのバージョンを削除したりするために、追加の認証要素が必要になります。MFA 削除により、万が一、セキュリティ認証が漏洩したり、不正なアクセスが行われた場合でも、セキュリティのレイヤーを追加することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1.5	S3バケットに「パブリックアクセスをブロックする (バケット設定) 」が設定されていることを確認する	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1.5	S3バケットに「パブリックアクセスをブロックする (バケット設定) 」が設定されていることを確認する	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
2.2.1	EBSボリュームの暗号化が有効であることを確認します	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.1	EBSボリュームの暗号化が有効であることを確認します	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2.3.1	RDSインスタンスで暗号化が有効であることを確認します	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.3.1	RDSインスタンスで暗号化が有効であることを確認します	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1	CloudTrail はすべてのリージョンで有効になっていることを確認します	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2	CloudTrailのログファイル検証が有効であることを確認する	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	CloudTrail ログの保存に使用されるS3 バケットが一般公開されていないことを確認します	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.3	CloudTrail ログの保存に使用されるS3 バケットが一般公開されていないことを確認します	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	CloudTrail ログの保存に使用されるS3 バケットが一般公開されていないことを確認します	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
3.4	CloudTrailトレイルが CloudWatchLogs と統合されていることを確認します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5	Config AWS がすべてのリージョンで有効になっていることを確認する	config-enabled-all-regions (Process Check)	Config AWS がすべての AWS リージョンで有効になっていることを確認します。コンソールの AWS Config セクション内で、有効なリージョンごとに AWS Config レコーダーが正しく設定されていることを確認します。グローバル AWS リソースのレコードが、少なくとも 1 つのリージョンで有効になっていることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6	S3 バケットアクセスログ記録が CloudTrail S3 バケットで有効になっていることを確認します	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
37	CloudTrail ログは保管時に KMS CMKs を使用して暗号化されていることを確認します	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
3.8	カスタマー作成の CMK のローテーションが有効になっていることを確認します	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。
3.9	すべての VPCs で VPC フローログ記録が有効になっていることを確認します	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	S3 バケットで書き込みイベントのオブジェクトレベルのログが有効になっていることを確認します	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
3.11	S3 バケットで書き込みイベントのオブジェクトレベルのログが有効になっていることを確認します	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します	alarm-unauthorized-api-calls (Process Check)	不正な API コールに対するログメトリクスフィルターとアラームが存在することを確認します このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2	MFA を使用しないマネジメントコンソールサインインに対してログメトリクスフィルターとアラームが存在することを確認します	alarm-sign-in-without-mfa (Process Check)	多要素認証 (MFA) を使用しない AWS マネジメントコンソールのサインインに対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.3	「ルート」アカウントに対してログメトリクスフィルターとアラームが存在することを確認します	alarm-root-account-use (Process Check)	ルートアカウントに対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4	MFA なしの IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認します。	alarm-iam-policy-change (Process Check)	IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.5	CloudTrail の設定の変更に対するログメトリクスフィルターとアラームが存在することを確認します。	alarm-cloudtrail-config-change (Process Check)	AWS CloudTrail 設定の変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	AWS マネジメントコンソールでの認証の失敗に対するログメトリクスフィルターとアラームが存在するようにする	alarm-console-auth-failures (Process Check)	AWS マネジメントコンソールでの認証の失敗に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.7	カスタマー作成の CMK の無効化またはスケジュールされた削除に対してログメトリクスフィルターとアラームが存在することを確認します	alarm-kms-disable-or-delete-cmk (Process Check)	顧客によって作成される CMK の無効化またはスケジュールされた削除に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8	S3 バケットの変更に対してログメトリクスフィルターとアラームが存在することを確認します	alarm-s3-bucket-policy-change (Process Check)	Amazon S3 バケットのポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.9	Config AWS 設定の変更に対してログメトリクスフィルターとアラームが存在することを確認する	alarm-aws-config-change (Process Check)	AWS Config の変更に対してログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.10	セキュリティグループの変更に対するメトリクスフィルターとアラームが存在することを確認します	alarm-vpc-secrity-group-change (Process Check)	セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認します このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.11	ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスとアラームが存在することを確認します	alarm-vpc-nacl-change (Process Check)	ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスフィルターとアラームが存在することを確認します このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.12	ネットワークゲートウェイへの変更に対するログメトリクスとアラームが存在することを確認します	alarm-vpc-network-gateway-change (Process Check)	ネットワークゲートウェイへの変更に対するログメトリクスとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.13	ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します	alarm-vpc-route-table-change (Process Check)	ルートテーブルの変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.14	VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します	alarm-vpc-change (Process Check)	Amazon Virtual Private Cloud (Amazon VPC) の変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.15	AWS Organizations の変更に対するログメトリクスフィルターとアラームが存在することを確認する	alarm-organizations-change (Process Check)	AWS Organizations の変更に対するログメトリクスフィルターとアラームが存在することを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.1	ネットワーク ACL が 0.0.0.0/0 からリモートサーバー管理ポートへの侵入を許可していないことを確認します	nacl-no-unrestricted-ssh-rdp	ネットワーク ACL で、リモートサーバーの管理ポートへのパブリック Ingress が許可されていないことを確認します。コンソールの [VPC] セクションで、ソースが「0.0.0.0/0」のネットワーク ACL があり、リモートサーバーの管理者ポートを含むポートまたはポート範囲が許可されていることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	ネットワーク ACL が 0.0.0.0/0 からリモートサーバー管理ポートへの侵入を許可していないことを確認します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	ネットワーク ACL が 0.0.0.0/0 からリモートサーバー管理ポートへの侵入を許可していないことを確認します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 ~ blockedPort5 パラメータ (CIS標準値: 3389) を任意に設定することができます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3	すべての VPC のデフォルトセキュリティグループがすべてのトラフィックを制限するようにします	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4	VPC ピアリングのルーティングテーブルが「アクセスが最も少ない」ことを確認します	vpc-peering-least-access (Process Check)	VPC ピアリングのルーティングテーブルが「最小限のアクセス」になっていることを確認します コンソールの [VPC] セクションで、ルートテーブルのエントリを確認し、ピアリングの目的を達成するために必要な最小限のサブネットまたはホストがルーティング可能であることを確認します。このコントロールの監査の詳細については、https://www.cisecurity.org/benchmark/amazon_web_services/ で入手可能な「CIS の Amazon Web Services Foundations Benchmark version 1.4.0」のドキュメントを参照してください

テンプレート

テンプレートは、GitHub の「Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2」で入手できます。

CIS の「Critical Security Controls v8 IG1」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Center for Internet Security (CIS) の「Critical Security Controls v8 IG1」と、 AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config は特定の AWS リソースに適用され、1 つ以上の CIS Critical Security Controls v8 IG1 コントロールに関連付けられます。CIS の「Critical Security Controls v8 IG1」によるコントロールを、複数の AWS Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-security-group-attached-to-eni	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。
2.2	認可されたソフトウェアが現在サポートされていることを確認する	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	認可されたソフトウェアが現在サポートされていることを確認する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	認可されたソフトウェアが現在サポートされていることを確認する	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 は AWS プラットフォームのバージョンを AWS パッチします。AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
3.3	データのアクセスコントロールリストを設定する	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.3	データのアクセスコントロールリストを設定する	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.3	データのアクセスコントロールリストを設定する	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
3.3	データのアクセスコントロールリストを設定する	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.3	データのアクセスコントロールリストを設定する	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
3.3	データのアクセスコントロールリストを設定する	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。
3.3	データのアクセスコントロールリストを設定する	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。
3.4	データ保持を実施する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	データ保持を実施する	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
4.1	安全な設定プロセスを確立および維持する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
4.1	安全な設定プロセスを確立および維持する	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
4.1	安全な設定プロセスを確立および維持する	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	エンタープライズアセットとソフトウェアを安全に管理する	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4.6	エンタープライズアセットとソフトウェアを安全に管理する	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4.6	エンタープライズアセットとソフトウェアを安全に管理する	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	エンタープライズアセットとソフトウェアを安全に管理する	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4.6	エンタープライズアセットとソフトウェアを安全に管理する	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	エンタープライズアセットとソフトウェアを安全に管理する	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
4.7	企業のアセットとソフトウェアのデフォルトアカウントを管理する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.1	アカウントのインベントリを確立および維持する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	一意のパスワードを使用する	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
5.2	一意のパスワードを使用する	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	一意のパスワードを使用する	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	一意のパスワードを使用する	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3	休眠アカウントを無効化する	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4	管理者権限を専用の管理者アカウントに限定する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4	管理者権限を専用の管理者アカウントに限定する	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4	リモートネットワークアクセスに対して MFA を要求する	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4	リモートネットワークアクセスに対して MFA を要求する	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4	リモートネットワークアクセスに対して MFA を要求する	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.5	管理者アクセスに対して MFA を要求する	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1	脆弱性管理プロセスを確立および維持する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1	脆弱性管理プロセスを確立および維持する	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1	脆弱性管理プロセスを確立および維持する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
7.3	自動化されたオペレーティングシステムのパッチ管理を実行する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3	自動化されたオペレーティングシステムのパッチ管理を実行する	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3	自動化されたオペレーティングシステムのパッチ管理を実行する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.4	自動化されたアプリケーションパッチ管理を実行する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
7.4	自動化されたアプリケーションパッチ管理を実行する	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.4	自動化されたアプリケーションパッチ管理を実行する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	監査ログの管理プロセスを確立および維持する	audit-log-policy-exists (Process check)	組織のログ要件を定義する、監査ログの管理ポリシーを確立して維持します。これには監査ログのレビューと保持が含まれますが、これらに限定されるわけではありません。
8.2	監査ログを収集する	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
8.2	監査ログを収集する	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
8.2	監査ログを収集する	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
8.2	監査ログを収集する	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
8.3	適切な監査ログのストレージを確保する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	マルウェア対策ソフトウェアのデプロイと維持	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2	マルウェア対策の署名の自動更新を設定する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
11.2	自動バックアップを実行する	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
11.2	自動バックアップを実行する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	リカバリデータを保護する	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.3	リカバリデータを保護する	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
11.3	リカバリデータを保護する	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	リカバリデータを保護する	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
11.4	リカバリデータの独立したインスタンスを確立して維持する	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
11.4	リカバリデータの独立したインスタンスを確立して維持する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for CIS Critical Security Controls v8 IG1」で入手できます。

CIS の「Critical Security Controls v8 IG2」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Center for Internet Security (CIS) の「Critical Security Controls v8 IG2」と、 AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config は特定の AWS リソースに適用され、1 つ以上の CIS Critical Security Controls v8 IG2 コントロールに関連付けられます。CIS Critical Security Controls v8 IG2 によるコントロールを、複数の AWS Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-security-group-attached-to-eni	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。
2.2	認可されたソフトウェアが現在サポートされていることを確認する	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	認可されたソフトウェアが現在サポートされていることを確認する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	認可されたソフトウェアが現在サポートされていることを確認する	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 は AWS プラットフォームのバージョンを AWS パッチします。AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.4	自動化されたソフトウェアインベントリツールを利用する	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.4	自動化されたソフトウェアインベントリツールを利用する	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
3.3	データのアクセスコントロールリストを設定する	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.3	データのアクセスコントロールリストを設定する	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.3	データのアクセスコントロールリストを設定する	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
3.3	データのアクセスコントロールリストを設定する	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.3	データのアクセスコントロールリストを設定する	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
3.3	データのアクセスコントロールリストを設定する	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。
3.3	データのアクセスコントロールリストを設定する	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。
3.4	データ保持を実施する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	データ保持を実施する	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
3.10	転送時に機密データを暗号化する	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.10	転送時に機密データを暗号化する	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.10	転送時に機密データを暗号化する	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.10	転送時に機密データを暗号化する	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
3.10	転送時に機密データを暗号化する	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
3.11	保管中の機密データを暗号化する	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
3.11	保管中の機密データを暗号化する	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
3.11	保管中の機密データを暗号化する	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
4.1	安全な設定プロセスを確立および維持する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
4.1	安全な設定プロセスを確立および維持する	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
4.1	安全な設定プロセスを確立および維持する	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	エンタープライズアセットとソフトウェアを安全に管理する	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4.6	エンタープライズアセットとソフトウェアを安全に管理する	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4.6	エンタープライズアセットとソフトウェアを安全に管理する	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	エンタープライズアセットとソフトウェアを安全に管理する	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4.6	エンタープライズアセットとソフトウェアを安全に管理する	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	エンタープライズアセットとソフトウェアを安全に管理する	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
4.7	企業のアセットとソフトウェアのデフォルトアカウントを管理する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.1	アカウントのインベントリを確立および維持する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	一意のパスワードを使用する	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
5.2	一意のパスワードを使用する	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	一意のパスワードを使用する	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	一意のパスワードを使用する	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3	休眠アカウントを無効化する	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4	管理者権限を専用の管理者アカウントに限定する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4	管理者権限を専用の管理者アカウントに限定する	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
5.6	アカウント管理を一元化する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4	リモートネットワークアクセスに対して MFA を要求する	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4	リモートネットワークアクセスに対して MFA を要求する	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4	リモートネットワークアクセスに対して MFA を要求する	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.5	管理者アクセスに対して MFA を要求する	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
6.7	アクセスコントロールを一元化する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1	脆弱性管理プロセスを確立および維持する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1	脆弱性管理プロセスを確立および維持する	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1	脆弱性管理プロセスを確立および維持する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
7.3	自動化されたオペレーティングシステムのパッチ管理を実行する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3	自動化されたオペレーティングシステムのパッチ管理を実行する	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3	自動化されたオペレーティングシステムのパッチ管理を実行する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.4	自動化されたアプリケーションパッチ管理を実行する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
7.4	自動化されたアプリケーションパッチ管理を実行する	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.4	自動化されたアプリケーションパッチ管理を実行する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.5	内部のエンタープライズアセットの脆弱性スキャンを自動的に実行する	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。
8.1	監査ログの管理プロセスを確立および維持する	audit-log-policy-exists (Process check)	組織のログ要件を定義する、監査ログの管理ポリシーを確立して維持します。これには監査ログのレビューと保持が含まれますが、これらに限定されるわけではありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
8.2	監査ログを収集する	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
8.2	監査ログを収集する	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
8.2	監査ログを収集する	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
8.3	適切な監査ログのストレージを確保する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
8.5	詳細な監査ログを収集する	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
8.5	詳細な監査ログを収集する	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
8.5	詳細な監査ログを収集する	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
8.5	詳細な監査ログを収集する	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.7	URL リクエストの監査ログを収集する	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
8.9	監査ログを一元管理する	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.10	監査ログを保持する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
8.10	監査ログを保持する	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	マルウェア対策ソフトウェアのデプロイと維持	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2	マルウェア対策の署名の自動更新を設定する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4	リムーバブルメディアのマルウェア対策の自動スキャンを設定する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6	マルウェア対策ソフトウェアを一元管理する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7	動作ベースのマルウェア対策ソフトウェアを使用する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
11.2	自動バックアップを実行する	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
11.2	自動バックアップを実行する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	リカバリデータを保護する	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.3	リカバリデータを保護する	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
11.3	リカバリデータを保護する	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	リカバリデータを保護する	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
11.4	リカバリデータの独立したインスタンスを確立して維持する	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
11.4	リカバリデータの独立したインスタンスを確立して維持する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
12.2	安全なネットワークアーキテクチャを確立および維持する	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
12.2	安全なネットワークアーキテクチャを確立および維持する	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
12.2	安全なネットワークアーキテクチャを確立および維持する	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
12.2	安全なネットワークアーキテクチャを確立および維持する	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
12.2	安全なネットワークアーキテクチャを確立および維持する	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
12.2	安全なネットワークアーキテクチャを確立および維持する	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	elbv2-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。
12.3	ネットワークインフラストラクチャを安全に管理する	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.3	ネットワークインフラストラクチャを安全に管理する	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
12.3	ネットワークインフラストラクチャを安全に管理する	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.3	ネットワークインフラストラクチャを安全に管理する	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
12.3	ネットワークインフラストラクチャを安全に管理する	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.3	ネットワークインフラストラクチャを安全に管理する	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
12.3	ネットワークインフラストラクチャを安全に管理する	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.3	ネットワークインフラストラクチャを安全に管理する	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
12.6	安全なネットワーク管理と通信プロトコルを使用する	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
12.6	安全なネットワーク管理と通信プロトコルを使用する	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.6	安全なネットワーク管理と通信プロトコルを使用する	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
12.6	安全なネットワーク管理と通信プロトコルを使用する	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.6	安全なネットワーク管理と通信プロトコルを使用する	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
12.6	安全なネットワーク管理と通信プロトコルを使用する	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.6	安全なネットワーク管理と通信プロトコルを使用する	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
12.6	安全なネットワーク管理と通信プロトコルを使用する	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.1	セキュリティイベントのアラートを一元化する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.1	セキュリティイベントのアラートを一元化する	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.3	ネットワーク侵入検知ソリューションをデプロイする	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.6	ネットワークトラフィックのフローログを収集する	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.6	ネットワークトラフィックのフローログを収集する	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、 AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for CIS Critical Security Controls v8 IG2」で入手できます。

CIS の「Critical Security Controls v8 IG3」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレート

としてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Center for Internet Security (CIS) の「Critical Security Controls v8 IG3」と AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config は特定の AWS リソースに適用され、1 つ以上の CIS Critical Security Controls v8 IG3 コントロールに関連付けられます。CIS の「Critical Security Controls v8 IG3」によるコントロールを、複数の AWS Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.1	詳細なエンタープライズアセットインベントリを確立して維持する	ec2-security-group-attached-to-eni	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。
2.2	認可されたソフトウェアが現在サポートされていることを確認する	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	認可されたソフトウェアが現在サポートされていることを確認する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	認可されたソフトウェアが現在サポートされていることを確認する	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 は AWS プラットフォームのバージョンを AWS パッチします。AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.4	自動化されたソフトウェアインベントリツールを利用する	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.4	自動化されたソフトウェアインベントリツールを利用する	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
3.3	データのアクセスコントロールリストを設定する	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.3	データのアクセスコントロールリストを設定する	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.3	データのアクセスコントロールリストを設定する	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
3.3	データのアクセスコントロールリストを設定する	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.3	データのアクセスコントロールリストを設定する	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
3.3	データのアクセスコントロールリストを設定する	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。
3.3	データのアクセスコントロールリストを設定する	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	データのアクセスコントロールリストを設定する	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。
3.4	データ保持を実施する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	データ保持を実施する	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
3.10	転送時に機密データを暗号化する	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.10	転送時に機密データを暗号化する	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.10	転送時に機密データを暗号化する	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.10	転送時に機密データを暗号化する	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
3.10	転送時に機密データを暗号化する	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.10	転送時に機密データを暗号化する	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
3.11	保管中の機密データを暗号化する	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
3.11	保管中の機密データを暗号化する	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
3.11	保管中の機密データを暗号化する	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.11	保管中の機密データを暗号化する	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11	保管中の機密データを暗号化する	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
3.14	機密データへのアクセスをログに記録する	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14	機密データへのアクセスをログに記録する	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14	機密データへのアクセスをログに記録する	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
3.14	機密データへのアクセスをログに記録する	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14	機密データへのアクセスをログに記録する	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
3.14	機密データへのアクセスをログに記録する	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14	機密データへのアクセスをログに記録する	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14	機密データへのアクセスをログに記録する	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
3.14	機密データへのアクセスをログに記録する	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14	機密データへのアクセスをログに記録する	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14	機密データへのアクセスをログに記録する	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14	機密データへのアクセスをログに記録する	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14	機密データへのアクセスをログに記録する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
3.14	機密データへのアクセスをログに記録する	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
4.1	安全な設定プロセスを確立および維持する	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
4.1	安全な設定プロセスを確立および維持する	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	安全な設定プロセスを確立および維持する	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	エンタープライズアセットとソフトウェアを安全に管理する	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4.6	エンタープライズアセットとソフトウェアを安全に管理する	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4.6	エンタープライズアセットとソフトウェアを安全に管理する	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	エンタープライズアセットとソフトウェアを安全に管理する	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4.6	エンタープライズアセットとソフトウェアを安全に管理する	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.6	エンタープライズアセットとソフトウェアを安全に管理する	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
4.7	企業のアセットとソフトウェアのデフォルトアカウントを管理する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.1	アカウントのインベントリを確立および維持する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	一意のパスワードを使用する	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
5.2	一意のパスワードを使用する	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	一意のパスワードを使用する	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	一意のパスワードを使用する	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3	休眠アカウントを無効化する	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4	管理者権限を専用の管理者アカウントに限定する	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4	管理者権限を専用の管理者アカウントに限定する	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
5.6	アカウント管理を一元化する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4	リモートネットワークアクセスに対して MFA を要求する	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4	リモートネットワークアクセスに対して MFA を要求する	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4	リモートネットワークアクセスに対して MFA を要求する	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.5	管理者アクセスに対して MFA を要求する	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
6.7	アクセスコントロールを一元化する	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1	脆弱性管理プロセスを確立および維持する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1	脆弱性管理プロセスを確立および維持する	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1	脆弱性管理プロセスを確立および維持する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
7.3	自動化されたオペレーティングシステムのパッチ管理を実行する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3	自動化されたオペレーティングシステムのパッチ管理を実行する	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3	自動化されたオペレーティングシステムのパッチ管理を実行する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.4	自動化されたアプリケーションパッチ管理を実行する	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
7.4	自動化されたアプリケーションパッチ管理を実行する	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.4	自動化されたアプリケーションパッチ管理を実行する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.5	内部のエンタープライズアセットの脆弱性スキャンを自動的に実行する	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。
8.1	監査ログの管理プロセスを確立および維持する	audit-log-policy-exists (Process check)	組織のログ要件を定義する、監査ログの管理ポリシーを確立して維持します。これには監査ログのレビューと保持が含まれますが、これらに限定されるわけではありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
8.2	監査ログを収集する	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
8.2	監査ログを収集する	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
8.2	監査ログを収集する	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2	監査ログを収集する	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
8.3	適切な監査ログのストレージを確保する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
8.5	詳細な監査ログを収集する	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
8.5	詳細な監査ログを収集する	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
8.5	詳細な監査ログを収集する	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.5	詳細な監査ログを収集する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
8.5	詳細な監査ログを収集する	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.7	URL リクエストの監査ログを収集する	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
8.9	監査ログを一元管理する	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.10	監査ログを保持する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
8.10	監査ログを保持する	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	マルウェア対策ソフトウェアのデプロイと維持	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2	マルウェア対策の署名の自動更新を設定する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4	リムーバブルメディアのマルウェア対策の自動スキャンを設定する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6	マルウェア対策ソフトウェアを一元管理する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7	動作ベースのマルウェア対策ソフトウェアを使用する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
11.2	自動バックアップを実行する	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	自動バックアップを実行する	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
11.2	自動バックアップを実行する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	リカバリデータを保護する	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.3	リカバリデータを保護する	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
11.3	リカバリデータを保護する	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	リカバリデータを保護する	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
11.4	リカバリデータの独立したインスタンスを確立して維持する	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	リカバリデータの独立したインスタンスを確立して維持する	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
11.4	リカバリデータの独立したインスタンスを確立して維持する	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
12.2	安全なネットワークアーキテクチャを確立および維持する	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
12.2	安全なネットワークアーキテクチャを確立および維持する	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
12.2	安全なネットワークアーキテクチャを確立および維持する	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
12.2	安全なネットワークアーキテクチャを確立および維持する	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
12.2	安全なネットワークアーキテクチャを確立および維持する	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
12.2	安全なネットワークアーキテクチャを確立および維持する	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.2	安全なネットワークアーキテクチャを確立および維持する	elbv2-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。
12.3	ネットワークインフラストラクチャを安全に管理する	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.3	ネットワークインフラストラクチャを安全に管理する	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
12.3	ネットワークインフラストラクチャを安全に管理する	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.3	ネットワークインフラストラクチャを安全に管理する	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
12.3	ネットワークインフラストラクチャを安全に管理する	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.3	ネットワークインフラストラクチャを安全に管理する	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
12.3	ネットワークインフラストラクチャを安全に管理する	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.3	ネットワークインフラストラクチャを安全に管理する	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
12.6	安全なネットワーク管理と通信プロトコルを使用する	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
12.6	安全なネットワーク管理と通信プロトコルを使用する	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.6	安全なネットワーク管理と通信プロトコルを使用する	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
12.6	安全なネットワーク管理と通信プロトコルを使用する	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.6	安全なネットワーク管理と通信プロトコルを使用する	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
12.6	安全なネットワーク管理と通信プロトコルを使用する	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.6	安全なネットワーク管理と通信プロトコルを使用する	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
12.6	安全なネットワーク管理と通信プロトコルを使用する	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.1	セキュリティイベントのアラートを一元化する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.1	セキュリティイベントのアラートを一元化する	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.3	ネットワーク侵入検知ソリューションをデプロイする	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.6	ネットワークトラフィックのフローログを収集する	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.6	ネットワークトラフィックのフローログを収集する	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13.10	アプリケーションレイヤーのフィルタリングを実行する	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、 AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。
16.1	安全なアプリケーション開発プロセスを確立および維持する	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16.12	コードレベルのセキュリティチェックを実装する	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16.12	コードレベルのセキュリティチェックを実装する	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、 AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
16.12	コードレベルのセキュリティチェックを実装する	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16.12	コードレベルのセキュリティチェックを実装する	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。
16.12	コードレベルのセキュリティチェックを実装する	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for CIS Critical Security Controls v8 IG3」で入手できます。

CIS の「Top 20」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するよう

には設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Center for Internet Security (CIS) の「Top 20 Critical Security Controls」と、 AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の CIS トップ 20 コントロールに関連付けられます。CIS の「Top 20」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックは、Payment Card Industry Qualified Security Assessors (QSAs)、HITRUST Certified Common Security Framework Practitioners (CCSFPs)、およびさまざまな業界フレームワークのガイダンスと評価を提供することを認定されたコンプライアンスプロフェッショナルのチームである AWS Security Assurance Services LLC (AWS SAS) によって検証されました。 AWS SAS プロフェッショナルは、お客様が CIS Top 20 のサブセットに合わせることができるようにこのコンフォーマンスパックを設計しました。

コントロール ID	AWS Config ルール	ガイダンス
CIS.2	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
CIS.2	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組

コントロール ID	AWS Config ルール	ガイダンス
		織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CIS.2	ec2-security-group-attached-to-eni	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。
CIS.2	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.2	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
CIS.2	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.3	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CIS.3	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.3	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
CIS.4	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CIS.4	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.4	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
CIS.4	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS Config ルール	ガイダンス
CIS.4	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.5	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
CIS.5	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.5	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CIS.5	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.5	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
CIS.6	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.6	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CIS.6	cloudtrail-enabled	AWS CloudTrail は、 マネジメントコンソールのアクションと API コールを記録 AWS することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.6	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性を確認します。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
CIS.6	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント の情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.6	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。
CIS.6	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.6	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CIS.6	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.6	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべてのから S3 バケット AWS リージョン にログファイルを配信します。さらに、 AWS が新しいリージョンを作成すると、CloudTrail はそのリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.6	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.6	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.6	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
CIS.6	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS Config ルール	ガイダンス
CIS.8	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CIS.9	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CIS.9	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CIS.9	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CIS.9	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。Amazon VPC 内に存在するドメインは論理的に隔離されているため、パブリックエンドポイントを使用するドメインよりも多くのセキュリティレイヤーが追加されています。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CIS.9	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
CIS.9	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CIS.9	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	s3-account-level-public-access-blocks	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
CIS.9	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CIS.9	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.9	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
CIS.9	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.10	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
CIS.10	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.10	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CIS.10	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.10	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
CIS.11	ec2-security-group-attached-to-eni	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.11	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
CIS.11	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.11	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
CIS.11	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CIS.12	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CIS.12	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
CIS.12	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CIS.12	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。Amazon VPC 内に存在するドメインは論理的に隔離されているため、パブリックエンドポイントを使用するドメインよりも多くのセキュリティレイヤーが追加されています。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CIS.12	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
CIS.12	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CIS.12	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	s3-account-level-public-access-blocks	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
CIS.12	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CIS.12	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
CIS.12	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.12	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
CIS.13	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.13	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CIS.13	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するには、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIS.13	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
CIS.13	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.13	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIS.13	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
CIS.13	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.13	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
CIS.13	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
CIS.13	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.13	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
CIS.13	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIS.13	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.13	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
CIS.13	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.13	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
CIS.13	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
CIS.13	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.13	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIS.13	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIS.13	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
CIS.14	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CIS.14	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するには、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
CIS.14	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
CIS.14	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CIS.14	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIS.14	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CIS.14	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
CIS.14	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。
CIS.14	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
CIS.14	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
CIS.14	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CIS.14	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIS.14	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CIS.14	s3-account-level-public-access-blocks	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
CIS.14	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
CIS.14	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CIS.14	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
CIS.14	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.14	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIS.14	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIS.14	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。
CIS.16	cloudtrail-enabled	AWS CloudTrail は、 マネジメントコンソールのアクションと API コールを記録 AWS することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CIS.16	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 および Centers for Internet Security (CIS) AWS Foundations Benchmark で説明されているパスワード強度に関する要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS Foundational Security Best Practices 値： true)、 RequireNumbers (AWS Foundational Security Best Practices 値： true)、 MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、 PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組

コントロール ID	AWS Config ルール	ガイダンス
		織のポリシーを反映する必要があります。
CIS.16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
CIS.16	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
CIS.16	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
CIS.16	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
CIS.16	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
CIS.16	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.16	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
CIS.16	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.18	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
CIS.18	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	AWS Config ルール	ガイダンス
CIS.19	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CIS.19	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS Config ルール	ガイダンス
CIS.19	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS Config ルール	ガイダンス
CIS.2	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for CIS Top 20」で入手できます。

CISA サイバーエッセンシャル 運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Cybersecurity & Infrastructure Security Agency (CISA) Cyber Essentials (CE) と AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の CISA CE コントロールに関連付けられます。CISA CE コントロール

は、複数の AWS Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
Your Staff-1 (お客様のスタッフ-1)	従業員がオンラインで適切な選択をするように奨励するため、意識を高める文化を育成します。	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
Your Staff-2 (お客様のスタッフ-2)	フィッシングやビジネスメールの侵害などのリスクについて学習します。XXXXX。	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
Your Staff-3 (お客様のスタッフ-3)	現在の脅威環境に対して常に警戒し、サイバーセキュリティの傾向に迅速に対応するために、教訓や報告を受けたイベントを活用して、サイバーセキュリティに	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	関連する現在のイベントに対する認識を維持します。		護する方法を従業員に教育するものです。
Your Staff-4 (お客様のスタッフ-4)	基本的なサイバーセキュリティトレーニングを活用して、サイバーセキュリティの概念、用語、サイバーセキュリティのベストプラクティスの実装に関連する活動について理解を深めます。	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
Your Staff-5 (お客様のスタッフ-5)	職能団体、学術機関、民間部門、政府機関を通じて利用可能なトレーニングリソースを特定します。	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
Your Systems-1	お客様のネットワークに誰がいるのかを知る。ハードウェアとソフトウェア資産のインベントリーを維持し、何が有効で、何が攻撃のリスクにさらされているかを把握する。	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
Your Systems-1	お客様のネットワークに誰がいるのかを知る。ハードウェアとソフトウェア資産のインベントリーを維持し、何が有効で、何が攻撃のリスクにさらされているかを把握する。	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
Your Systems-1	お客様のネットワークに誰がいるのかを知る。ハードウェアとソフトウェア資産のインベントリーを維持し、何が有効で、何が攻撃のリスクにさらされているかを把握する。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
Your Systems-1	お客様のネットワークに誰がいるのかを知る。ハードウェアとソフトウェア資産のインベントリーを維持し、何が有効で、何が攻撃のリスクにさらされているかを把握する。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
Your Systems-1	お客様のネットワークに誰がいるのかを知る。ハードウェアとソフトウェア資産のインベントリーを維持し、何が有効で、何が攻撃のリスクにさらされているかを把握する。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
Your Systems-1	お客様のネットワークに誰がいるのかを知る。ハードウェアとソフトウェア資産のインベントリーを維持し、何が有効で、何が攻撃のリスクにさらされているかを把握する。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
Your Systems-1	お客様のネットワークに誰がいるのかを知る。ハードウェアとソフトウェア資産のインベントリーを維持し、何が有効で、何が攻撃のリスクにさらされているかを把握する。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-2	すべての OS とサードパーティソフトウェアの自動アップデートを活用する。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
お客様のシステム-2	すべての OS とサードパーティソフトウェアの自動アップデートを活用する。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-2	すべての OS とサードパーティソフトウェアの自動アップデートを活用する。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-2	すべての OS とサードパーティソフトウェアの自動アップデートを活用する。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	api-gw-execution-logging-enabled	API Gateway の口グ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) では、高可用性と耐障害性のために少なくとも 3 つのデータノードが必要です。少なくとも 3 つのデータノードを持つ OpenSearch Service ドメインをデプロイすると、ノードに障害が発生した場合のクラスターオペレーションが確実になります。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	secretsmanager-secret-periodic-rotation	このルールにより、 AWS Secrets Manager シークレットで定期的なローテーションが有効になっていることが保証されます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-3	すべてのハードウェアおよびソフトウェア資産にセキュリティ設定を実施する。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のシステム-4	サポートされていない、または許可されていないハードウェアやソフトウェアをシステムから削除します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の周囲環境-1	お客様のネットワークに誰がいるのかを知る。ネットワーク接続 (ユーザー、ベンダー、ビジネスパートナーなど) のインベントリーを維持してください。	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
お客様の周囲環境-1	お客様のネットワークに誰がいるのかを知る。ネットワーク接続 (ユーザー、ベンダー、ビジネスパートナーなど) のインベントリーを維持してください。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の周囲環境-1	お客様のネットワークに誰がいるのかを知る。ネットワーク接続 (ユーザー、ベンダー、ビジネスパートナーなど) のインベントリーを維持してください。	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。
Your Surroundings-2	特権ユーザー、管理者ユーザー、リモートアクセスユーザーをはじめ、すべてのユーザーに対して多要素認証を活用する。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
Your Surroundings-2	特権ユーザー、管理者ユーザー、リモートアクセスユーザーをはじめ、すべてのユーザーに対して多要素認証を活用する。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
Your Surroundings-2	特権ユーザー、管理者ユーザー、リモートアクセスユーザーをはじめ、すべてのユーザーに対して多要素認証を活用する。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
Your Surroundings-2	特権ユーザー、管理者ユーザー、リモートアクセスユーザーをはじめ、すべてのユーザーに対して多要素認証を活用する。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の周囲環境-3	必要最小限の権限に基づき、アクセス権限と管理者権限を付与します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の周囲環境-3	必要最小限の権限に基づき、アクセス権限と管理者権限を付与します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
お客様の周囲環境-3	必要最小限の権限に基づき、アクセス権限と管理者権限を付与します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の周囲環境-3	必要最小限の権限に基づき、アクセス権限と管理者権限を付与します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の周囲環境-3	必要最小限の権限に基づき、アクセス権限と管理者権限を付与します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の周囲環境-3	必要最小限の権限に基づき、アクセス権限と管理者権限を付与します。	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の周囲環境-3	必要最小限の権限に基づき、アクセス権限と管理者権限を付与します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の周囲環境-4	すべてのユーザーに一意のパスワードを活用します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のデータ-1	お客様のデータがどのように保護されているか、ご覧ください。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-2	ネットワークと境界のコンポーネント、ホストとデバイスのコンポーネント、静止データと転送中のデータ、ユーザーの行動アクティビティを管理します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-3	ドメインネームシステムの保護。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンスが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-4	主要システムの定期的な自動バックアップと冗長化を確立します。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
お客様のデータ-5	物理的なセキュリティ、暗号化、オフラインコピーなど、バックアップのための保護機能を活用します。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様のデータ-5	物理的なセキュリティ、暗号化、オフラインコピーなど、バックアップのための保護機能を活用します。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
お客様の危機管理-2	攻撃を検知し、伝達し、封じ込めるための内部報告体制の整備をリードします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
お客様の危機管理-2	攻撃を検知し、伝達し、封じ込めるための内部報告体制の整備をリードします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-1	重要なデータやシステム構成を自動的かつ継続的にバックアップするソリューションを採用します。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-2	可能な限り、システムへのアクセスに多要素認証 (MFA) を要求します。 MFA はすべてのユーザーに必要ですが、まずは特権ユーザー、管理者ユーザー、リモートアクセスユーザーから始めましょう。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-2	可能な限り、システムへのアクセスに多要素認証 (MFA) を要求します。 MFA はすべてのユーザーに必要ですが、まずは特権ユーザー、管理者ユーザー、リモートアクセスユーザーから始めましょう。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-2	可能な限り、システムへのアクセスに多要素認証 (MFA) を要求します。 MFA はすべてのユーザーに必要ですが、まずは特権ユーザー、管理者ユーザー、リモートアクセスユーザーから始めましょう。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-2	可能な限り、システムへのアクセスに多要素認証 (MFA) を要求します。 MFA はすべてのユーザーに必要ですが、まずは特権ユーザー、管理者ユーザー、リモートアクセスユーザーから始めましょう。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-3	可能な限り、自動アップデートを有効にする。サポートされていない OS、アプリケーション、ハードウェアを交換する。パッチのテストとデプロイを迅速に行います。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
ブートアップ: 最初にやるべきこと-3	可能な限り、自動アップデートを有効にする。サポートされていない OS、アプリケーション、ハードウェアを交換する。パッチのテストとデプロイを迅速に行います。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-3	可能な限り、自動アップデートを有効にする。サポートされていない OS、アプリケーション、ハードウェアを交換する。パッチのテストとデプロイを迅速に行います。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ブートアップ: 最初にやるべきこと-3	可能な限り、自動アップデートを有効にする。サポートされていない OS、アプリケーション、ハードウェアを交換する。パッチのテストとデプロイを迅速に行います。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for CISA Cyber Essentials」で入手できます。

Criminal Justice Information Services (CJIS) の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Criminal Justice Information Services (CJIS) コンプライアンス要件と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の CJIS コントロールに関連付けられます。CJIS によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.2	セキュリティ意識向上トレーニング	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
5.3	インシデントへの対応	response-plan-exists-maintained (Process Check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。正式にドキュメント化された更新済みの対応計画を用意することで、対応する担当者がイ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ンシデントの発生中に従うべき役割、責任、プロセスを理解することができます。
5.3	インシデントへの対応	response-plan-tested (Process Check)	インシデント対応と復旧計画がテスト済みであることを確認します。これにより、インシデント発生時に計画が有効であるか、ギャップや更新に対処する必要があるかどうかを理解することができます。
5.4	監査と説明責任	audit-log-policy-exists (Process check)	組織のログ要件を定義する、監査ログの管理ポリシーを確立して維持します。これには監査ログのレビューと保持が含まれますが、これらに限定されるわけではありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
5.4.1	監査可能なイベントとコンテンツ (情報システム)	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
5.4.1	監査可能なイベントとコンテンツ (情報システム)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
5.4.1	監査可能なイベントとコンテンツ (情報システム)	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
5.4.1	監査可能なイベントとコンテンツ (情報システム)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
5.4.1	監査可能なイベントとコンテンツ (情報システム)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.1	監査可能なイベントとコンテンツ (情報システム)	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。
5.4.5	監査情報の保護	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.5	監査情報の保護	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
5.4.5	監査情報の保護	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.4.6	監査記録の保持	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
5.4.6	監査記録の保持	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで IAM パスワードポリシーに RequireUppercaseCharacters (CJIS 値: false)、RequireLowercaseCharacters (CJIS 値: false)、RequireSymbols (CJIS 値: false)、RequireNumbers (CJIS 値: false)、MinimumPasswordLength (CJIS 値: 8)、PasswordReusePrevention (CJIS 値: 10)、MaxPasswordAge (CJIS 値: 90) を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
5.5.2	アクセスの実施	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
5.5.2	アクセスの実施	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	rds-instance-iam-authentication-enabled	システムおよびアセットへのアクセスを制御するために、Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。これにより、データベースに出入りするネットワークトラフィックが、Secure Sockets Layer (SSL) を使用して暗号化されるようになります。認証は外部で管理されるため、ユーザー認証情報をデータベースに保存する必要はありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2	アクセスの実施	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。
5.5.2.1	最小特権	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
5.5.2.1	最小特権	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。
5.5.2.1	最小特権	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。
5.5.2.1	最小特権	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.2.1	最小特権	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.6	リモートアクセス	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.5.6	リモートアクセス	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.6.2.1.1	パスワード	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで IAM パスワードポリシーに RequireUppercaseCharacters (CJIS 値: false)、RequireLowercaseCharacters (CJIS 値: false)、RequireSymbols (CJIS 値: false)、RequireNumbers (CJIS 値: false)、MinimumPasswordLength (CJIS 値: 8)、PasswordReusePrevention (CJIS 値: 10)、MaxPasswordAge (CJIS 値: 90) を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.6.2.2	高度な認証	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.6.2.2	高度な認証	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.6.2.2	高度な認証	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.6.2.2	高度な認証	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.6.2.2	高度な認証	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.6.3.1	識別子の管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
5.7.1.1	最小の機能	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
5.7.1.1	最小の機能	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
5.7.1.1	最小の機能	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
5.7.1.1	最小の機能	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
5.7.1.1	最小の機能	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
5.7.1.1	最小の機能	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.7.1.1	最小の機能	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
5.10	システムと通信の保護と情報の整合性	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10	システムと通信の保護と情報の整合性	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10	システムと通信の保護と情報の整合性	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10	システムと通信の保護と情報の整合性	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10	システムと通信の保護と情報の整合性	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10	システムと通信の保護と情報の整合性	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10	システムと通信の保護と情報の整合性	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10	システムと通信の保護と情報の整合性	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10	システムと通信の保護と情報の整合性	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10	システムと通信の保護と情報の整合性	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10	システムと通信の保護と情報の整合性	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10	システムと通信の保護と情報の整合性	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。
5.10	システムと通信の保護と情報の整合性	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10.1	情報フローの実施	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10.1	情報フローの実施	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10.1	情報フローの実施	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
5.10.1	情報フローの実施	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
5.10.1	情報フローの実施	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10.1	情報フローの実施	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
5.10.1	情報フローの実施	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
5.10.1	情報フローの実施	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1	情報フローの実施	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.1	境界保護	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.1	境界保護	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.1	境界保護	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
5.10.1.1	境界保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.1	境界保護	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.1	境界保護	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.1	境界保護	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
5.10.1.1	境界保護	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.1	境界保護	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。
5.10.1.1	境界保護	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。
5.10.1.1	境界保護	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10.1.2	Encryption	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
5.10.1.2	Encryption	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
5.10.1.2	Encryption	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
5.10.1.2	Encryption	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。
5.10.1.2	Encryption	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
5.10.1.2	Encryption	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
5.10.1.2	Encryption	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10.1.2	Encryption	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
5.10.1.2	Encryption	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
5.10.1.2	Encryption	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
5.10.1.2	Encryption	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10.1.2	Encryption	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
5.10.1.2	Encryption	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
5.10.1.2	Encryption	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
5.10.1.2	Encryption	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
5.10.1.2	Encryption	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.2	Encryption	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
5.10.1.2	Encryption	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.3	侵入検知ツールとテクニック	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.3	侵入検知ツールとテクニック	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.1.3	侵入検知ツールとテクニック	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.4.1	パッチ管理	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.4.1	パッチ管理	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.4.1	パッチ管理	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.4.1	パッチ管理	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。 AWS Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 はプラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.4.1	パッチ管理	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.4.4	セキュリティアラートとアドバイザリ	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.4.4	セキュリティアラートとアドバイザリ	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.10.4.4	セキュリティアラートとアドバイザリ	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

テンプレート

テンプレートは、GitHub の「CJIS の運用のベストプラクティス」で入手できます。

CMMC 2.0 Level 1 に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するよう

には設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1 と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の CMMC 2.0 Level 1 コントロールに関連付けられます。「CMMC 2.0 Level 1」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			シーを反映する必要があります。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L1-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
IA.L1-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
IA.L1-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA.L1-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L1-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L1-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L1-3.14.1	情報および情報システムの欠陥をタイムリーに特定、報告して修正します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L1-3.14.1	情報および情報システムの欠陥をタイムリーに特定、報告して修正します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L1-3.14.1	情報および情報システムの欠陥をタイムリーに特定、報告して修正します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L1-3.14.2	組織の情報システム内の適切な場所で、悪意のあるコードから保護します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
SI.L1-3.14.5	ファイルがダウンロード、開く、または実行されるときに、情報システムの定期的なスキャンを実行し、外部ソースからのファイルのリアルタイムスキャンを実行します。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for CMMC 2.0 Level 1」(CMMC 2.0 Level 1 に関する運用上のベストプラクティス) で入手できます。

CMMC 2.0 Level 2 に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、「Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2」と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の CMMC 2.0 Level 2 コントロールに関連付けられます。CMMC 2.0 Level 2 によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.1	情報システムへのアクセスを、権限のあるユーザーと、権限のあるユーザーに代わって動作するプロセスまたはデバイス (他の情報システムを含む) に制限します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.2	情報システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.20	外部の情報システムへの接続と使用を検証して制御/制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.3	承認された認可に従って CUI のフローをコントロールします。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.7	権限のないユーザーが権限が必要な機能を実行できないようにし、それらの機能の実行を監査ログに記録します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AC.L2-3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC.L2-3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.1	違法または不正なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査ログと監査レコードを作成し、保持します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU.L2-3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU.L2-3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.4	監査ログのプロセスに障害が発生した場合に、アラートを生成します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.4	監査ログのプロセスに障害が発生した場合に、アラートを生成します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU.L2-3.3.4	監査ログのプロセスに障害が発生した場合に、アラートを生成します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.4	監査ログのプロセスに障害が発生した場合に、アラートを生成します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.5	監査記録のレビュー、分析、報告プロセスを相関させて調査し、違法、未許可、疑わしい、または異常なアクティビティの兆候に対応します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.5	監査記録のレビュー、分析、報告プロセスを相関させて調査し、違法、未許可、疑わしい、または異常なアクティビティの兆候に対応します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU.L2-3.3.8	監査情報と監査ログ記録ツールを、不正なアクセス、変更、削除から保護します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
CA.L2-3.12.2	組織システムの欠陥を修正し、脆弱性を低減または排除するために設計された行動計画を策定し、実施します。	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。これには、脆弱性管理ツール、環境スキャンの周期、役割と責任などが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA.L2-3.12.3	セキュリティコントロールを継続的にモニタリングし、そのコントロールの継続的な有効性を確認します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA.L2-3.12.3	セキュリティコントロールを継続的にモニタリングし、そのコントロールの継続的な有効性を確認します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA.L2-3.12.3	セキュリティコントロールを継続的にモニタリングし、そのコントロールの継続的な有効性を確認します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CM.L2-3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.2	組織のシステムに採用される、情報テクノロジーを使用した製品のセキュリティ構成の設定を確立して実施します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、および ログの記録を実行します。	api-gw-execution-logging-enabled	API Gateway の ログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、および ログの記録を実行します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.3	組織のシステムに対する変更の追跡、レビュー、承認、不承認、およびログの記録を実行します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.7	重要性のないプログラム、機能、ポート、プロトコル、サービスの使用を制限、無効化、または防止します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.9	ユーザーがインストールしたソフトウェアをコントロールおよびモニタリングします。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.9	ユーザーがインストールしたソフトウェアをコントロールおよびモニタリングします。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM.L2-3.4.9	ユーザーがインストールしたソフトウェアをコントロールおよびモニタリングします。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
IA.L2-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
IA.L2-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.1	情報システムのユーザーと、ユーザーに代わって動作するプロセスまたはデバイスを特定します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA.L2-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.2	組織の情報システムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.3	権限のあるアカウントへのローカルおよびネットワークアクセスと、権限のないアカウントへのネットワークアクセスに、多要素認証を使用します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.3	権限のあるアカウントへのローカルおよびネットワークアクセスと、権限のないアカウントへのネットワークアクセスに、多要素認証を使用します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.3	権限のあるアカウントへのローカルおよびネットワークアクセスと、権限のないアカウントへのネットワークアクセスに、多要素認証を使用します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.3	権限のあるアカウントへのローカルおよびネットワークアクセスと、権限のないアカウントへのネットワークアクセスに、多要素認証を使用します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.6	定義されたアイドル状態の期間を経過したときに、識別子を無効にします。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.6	定義されたアイドル状態の期間を経過したときに、識別子を無効にします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.7	新しいパスワードが作成される際、パスワードの複雑さと文字の変更を最小限に抑えます。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.8	指定した世代数でのパスワードの再利用を禁止します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA.L2-3.5.10	暗号で保護されたパスワードのみを保存および転送します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
IR.L2-3.6.1	準備、検出、分析、抑制、回復、およびユーザーの応答アクティビティなど、組織のシステムで運用するインシデント処理機能を確立します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR.L2-3.6.1	準備、検出、分析、抑制、回復、およびユーザーの応答アクティビティなど、組織のシステムで運用するインシデント処理機能を確立します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
IR.L2-3.6.1	準備、検出、分析、抑制、回復、およびユーザーの応答アクティビティなど、組織のシステムで運用するインシデント処理機能を確立します。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR.L2-3.6.1	準備、検出、分析、抑制、回復、およびユーザーの応答アクティビティなど、組織のシステムで運用するインシデント処理機能を確立します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR.L2-3.6.3	組織のインシデント対応能力をテストします。	response-plan-tested (Process Check)	インシデント対応と復旧計画がテスト済みであることを確認します。これにより、インシデント発生時に計画が有効であるか、ギャップや更新に対処する必要があるかどうかを理解することができます。
MA.L2-3.7.5	外部ネットワーク接続から、ローカル以外でのメンテナンスセッションを確立し、ローカル以外でのメンテナンスが完了したときにその接続を終了するには、多要素認証が必要です。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
MA.L2-3.7.5	外部ネットワーク接続から、ローカル以外でのメンテナンスセッションを確立し、ローカル以外でのメンテナンスが完了したときにその接続を終了するには、多要素認証が必要です。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA.L2-3.11.2	組織のシステムやアプリケーションの脆弱性を定期的にスキャンし、それらのシステムやアプリケーションに影響を与える新たな脆弱性が発見された場合には、その脆弱性をスキャンします。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
RA.L2-3.11.2	組織のシステムやアプリケーションの脆弱性を定期的にスキャンし、それらのシステムやアプリケーションに影響を与える新たな脆弱性が発見された場合には、その脆弱性をスキャンします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA.L2-3.11.2	組織のシステムやアプリケーションの脆弱性を定期的にスキャンし、それらのシステムやアプリケーションに影響を与える新たな脆弱性が発見された場合には、その脆弱性をスキャンします。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA.L2-3.11.2	組織のシステムやアプリケーションの脆弱性を定期的にスキャンし、それらのシステムやアプリケーションに影響を与える新たな脆弱性が発見された場合には、その脆弱性をスキャンします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.1	情報システムの外部境界および主要な内部境界で、組織レベルの通信 (組織の情報システムによって送受信される情報など) をモニタリング、コントロールして保護します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.4	共有システムリソースからの、未許可の意図しない情報転送を防止します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.10	組織のシステムで採用されている暗号化で使用する暗号化キーを設定して管理します。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.10	組織のシステムで採用されている暗号化で使用する暗号化キーを設定して管理します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
SC.L2-3.13.15	通信のセッションの信頼性を確保します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.15	通信のセッションの信頼性を確保します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
SC.L2-3.13.15	通信のセッションの信頼性を確保します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.15	通信のセッションの信頼性を確保します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC.L2-3.13.15	通信のセッションの信頼性を確保します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.15	通信のセッションの信頼性を確保します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC.L2-3.13.16	保管中の CUI の機密性を確保します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.1	情報および情報システムの欠陥をタイムリーに特定、報告して修正します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.1	情報および情報システムの欠陥をタイムリーに特定、報告して修正します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.1	情報および情報システムの欠陥をタイムリーに特定、報告して修正します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.2	組織の情報システム内の適切な場所で、悪意のあるコードから保護します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
SI.L2-3.14.5	ファイルがダウンロード、開く、または実行されるときに、情報システムの定期的なスキャンを実行し、外部ソースからのファイルのリアルタイムスキャンを実行します。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
SI.L2-3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
SI.L2-3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI.L2-3.14.7	組織のシステムの不正使用を特定します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for CMMC 2.0 Level 2」(CMMC 2.0 Level 2 に関する運用上のベストプラクティス) で入手できます。

コンピューティングサービスに関する運用上のベストプラクティス

このコンフォーマンスパックには、コンピューティングサービスに基づく AWS Config ルールが含まれています。詳細については、「あらゆるワークロードのためのコンピューティング」を参照してください。でサポートされているすべてのマネージドルールのリストについては AWS Config、「AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Compute Services」で入手できます。

データの回復性に関する運用上のベストプラクティス

でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Data Resiliency」で入手できます。

データベースサービスに関する運用上のベストプラクティス

このコンフォーマンスパックには、 Databases Services に基づく AWS Config ルールが含まれています。詳細については、「 のデータベース AWS」を参照してください。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Databases Services」で入手できます。

データレイクと分析サービスに関する運用上のベストプラクティス

このコンフォーマンスパックには、データレイクと分析サービスの AWS Config ルールが含まれています。詳細については、「Data Lakes and Analytics on AWS」を参照してください。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Data Lakes and Analytics Services」で入手できます。

DevOP s 運用のベストプラクティス

このコンフォーマンスパックには、DevOps に基づく AWS Config ルールが含まれています AWS。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for DevOps」で入手できます。

EC2 に関する運用上のベストプラクティス

このコンフォーマンスパックには、EC2 に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for EC2」で入手できます。

暗号化とキー管理に関する運用上のベストプラクティス

でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Encryption and Key Management」で入手できます。

SME 向け ENISA サイバーセキュリティガイドの運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するよう

には設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、欧州連合サイバーセキュリティ庁 (ENISA) の SMEs 向けサイバーセキュリティガイドと AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、SMEs。SME 向け ENISA サイバーセキュリティガイドの 1 つのコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックのサンプルテンプレートには、SME 向け ENISA サイバーセキュリティガイドから適合されたコントロールへのマッピングが含まれています。SME 向け ENISA サイバーセキュリティガイドは、「Cybersecurity guide for SMEs - 12 steps to securing your business」から入手できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_DEVELOP GOOD CYBERSECURITY CULTURE: PUBLISH CYBERSECURITY POLICIES (1_優れたサイバーセキュリティ文化を育成する:サイバーセキュリティポリシーを公開)	サイバーセキュリティでは、明確かつ具体的なルールを概説する必要があります	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。		リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elasticsearch Service (Amazon ES) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	elasticsearch-node-to-node-encryption-check	Amazon Elasticsearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1_優れたサイバーセキュリティ文化の構築: データ保護を忘れない	EU 一般データ保護規則 1 に基づき、EU/EEA 居住者の個人データを処理または保存するすべての中小企業は、そのデータを保護するために適切なセキュリティコントロールが実施されていることを確認する必要があります。この中には、中小企業の代理として働く第三者が適切なセキュリティ対策を講じていることを保証することも含まれます。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2_適切なトレーニングを提供する	すべての従業員がサイバーセキュリティのさまざまな脅威を認識して対処できるように、従業員に対して定期的にサイバーセキュリティ意識トレーニングを実施します。これらのトレーニングは中小企業に合わせて調整され、実際の状況に焦点を当てたものである必要があります。社内のサイバーセキュリティを管理する責任者に専門的なサイバーセキュリティトレーニングを行い、業務遂行に必要なスキルとコンピテンシーを確保できるようにします。	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4_インシデント対応計画を作成する	正式なインシデント対応計画を作成します。この計画では、すべてのセキュリティインシデントに専門的かつ適切な方法でタイムリーに対応できるようにするための明確なガイドライン、役割、および責任を文書化します。セキュリティの脅威に迅速に対応するために、疑わしいアクティビティやセキュリティ違反を監視して違反発生時にアラートを作成できるツールについて調査します。	response-plan-exists-maintained (Process Check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5_システムへの安全なアクセス	すべての人に対して、少なくとも 3 つのランダムな一般的な単語を組み合わせた、覚えやすさとセキュリティの両方で非常に優れたパスフレーズを使用するよう奨励してください。一般的なパスワードを選択した場合：-小文字と大文字、場合によっては数字と特殊文字を使用して長くしてください。-「password」のような簡単すぎるフレーズ、「abc」や「123」のような連続した文字や数字は避けてください。-オンライン上で入手できる個人情報の使用は避けてください。またパスフレーズやパスワードを使用する際は、決して他の場所で再利用しないでください。- 同僚と共有しないでください。- 多要素認証を有効化します。-専用のパスワードマ	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ネージャーを使用します。		のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5_システムへの安全なアクセス	すべての人に対して、少なくとも 3 つのランダムな一般的な単語を組み合わせた、覚えやすさとセキュリティの両方で非常に優れたパスフレーズを使用するよう奨励してください。一般的なパスワードを選択した場合：-小文字と大文字、場合によっては数字と特殊文字を使用して長くしてください。-「password」のような簡単すぎるフレーズ、「abc」や「123」のような連続した文字や数字は避けてください。-オンライン上で入手できる個人情報の使用は避けてください。またパスフレーズやパスワードを使用する際は、決して他の場所で再利用しないでください。- 同僚と共有しないでください。- 多要素認証を有効化します。-専用のパスワードマ	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ネージャーを使用します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5_システムへの安全なアクセス	すべての人に対して、少なくとも 3 つのランダムな一般的な単語を組み合わせた、覚えやすさとセキュリティの両方で非常に優れたパスフレーズを使用するよう奨励してください。一般的なパスワードを選択した場合：-小文字と大文字、場合によっては数字と特殊文字を使用して長くしてください。-「password」のような簡単すぎるフレーズ、「abc」や「123」のような連続した文字や数字は避けてください。-オンライン上で入手できる個人情報の使用は避けてください。またパスフレーズやパスワードを使用する際は、決して他の場所で再利用しないでください。- 同僚と共有しないでください。- 多要素認証を有効化します。-専用のパスワードマ	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ネージャーを使用します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5_システムへの安全なアクセス	すべての人に対して、少なくとも 3 つのランダムな一般的な単語を組み合わせた、覚えやすさとセキュリティの両方で非常に優れたパスフレーズを使用するよう奨励してください。一般的なパスワードを選択した場合：-小文字と大文字、場合によっては数字と特殊文字を使用して長くしてください。-「password」のような簡単すぎるフレーズ、「abc」や「123」のような連続した文字や数字は避けてください。-オンライン上で入手できる個人情報の使用は避けてください。またパスフレーズやパスワードを使用する際は、決して他の場所で再利用しないでください。- 同僚と共有しないでください。- 多要素認証を有効化します。-専用のパスワードマ	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ネージャーを使用します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5_システムへの安全なアクセス	すべての人に対して、少なくとも 3 つのランダムな一般的な単語を組み合わせた、覚えやすさとセキュリティの両方で非常に優れたパスフレーズを使用するよう奨励してください。一般的なパスワードを選択した場合：-小文字と大文字、場合によっては数字と特殊文字を使用して長くしてください。-「password」のような簡単すぎるフレーズ、「abc」や「123」のような連続した文字や数字は避けてください。-オンライン上で入手できる個人情報の使用は避けてください。またパスフレーズやパスワードを使用する際は、決して他の場所で再利用しないでください。- 同僚と共有しないでください。- 多要素認証を有効化します。-専用のパスワードマ	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ネージャーを使用します。		
6_デバイスのセキュリティ確保: ソフトウェアにパッチを適用し、最新の状態に保つ	集中型プラットフォームを使用してパッチ適用を管理するのが理想的です。中小企業には、次のことを強くお勧めします。- すべてのソフトウェアを定期的に更新してください。- 可能な限り、自動アップデートを有効にしてください。- 手動更新が必要なソフトウェアとハードウェアを特定します。- モバイルおよび IoT デバイスを考慮してください。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: ソフトウェアにパッチを適用し、最新の状態に保つ	集中型プラットフォームを使用してパッチ適用を管理するのが理想的です。中小企業には、次のことを強くお勧めします。- すべてのソフトウェアを定期的に更新してください。- 可能な限り、自動アップデートを有効にしてください。- 手動更新が必要なソフトウェアとハードウェアを特定します。- モバイルおよび IoT デバイスを考慮してください。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: ソフトウェアにパッチを適用し、最新の状態に保つ	集中型プラットフォームを使用してパッチ適用を管理するのが理想的です。中小企業には、次のことを強くお勧めします。- すべてのソフトウェアを定期的に更新してください。- 可能な限り、自動アップデートを有効にしてください。- 手動更新が必要なソフトウェアとハードウェアを特定します。- モバイルおよび IoT デバイスを考慮してください。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: ソフトウェアにパッチを適用し、最新の状態に保つ	集中型プラットフォームを使用してパッチ適用を管理するのが理想的です。中小企業には、次のことを強くお勧めします。- すべてのソフトウェアを定期的に更新してください。- 可能な限り、自動アップデートを有効にしてください。- 手動更新が必要なソフトウェアとハードウェアを特定します。- モバイルおよび IoT デバイスを考慮してください。	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。 AWS Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 はプラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: ソフトウェアにパッチを適用し、最新の状態に保つ	集中型プラットフォームを使用してパッチ適用を管理するのが理想的です。中小企業には、次のことを強くお勧めします。- すべてのソフトウェアを定期的に更新してください。- 可能な限り、自動アップデートを有効にしてください。- 手動更新が必要なソフトウェアとハードウェアを特定します。- モバイルおよび IoT デバイスを考慮してください。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: ソフトウェアにパッチを適用し、最新の状態に保つ	集中型プラットフォームを使用してパッチ適用を管理するのが理想的です。中小企業には、次のことを強くお勧めします。- すべてのソフトウェアを定期的に更新してください。- 可能な限り、自動アップデートを有効にしてください。- 手動更新が必要なソフトウェアとハードウェアを特定します。- モバイルおよび IoT デバイスを考慮してください。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: ソフトウェアにパッチを適用し、最新の状態に保つ	集中型プラットフォームを使用してパッチ適用を管理するのが理想的です。中小企業には、次のことを強くお勧めします。- すべてのソフトウェアを定期的に更新してください。- 可能な限り、自動アップデートを有効にしてください。- 手動更新が必要なソフトウェアとハードウェアを特定します。- モバイルおよび IoT デバイスを考慮してください。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	[api-gw-cache-enabled-and-encrypted](#)	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elasticsearch Service (Amazon ES) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	elasticsearch-node-to-node-encryption-check	Amazon Elasticsearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6_デバイスのセキュリティ確保: 暗号化	データを暗号化して保護します。中小企業では、ノートパソコン、スマートフォン、タブレットなどのモバイルデバイスに保存されているデータを確実に暗号化する必要があります。ホテルや空港の WiFi ネットワークなどの公開ネットワーク経由で転送されるデータについては、バーチャルプライベートネットワーク (VPN) を使用するか、SSL/TLS プロトコルを使用した安全な接続を介してウェブサイトにアクセスすることにより、データが確実に暗号化されるようにします。インターネット経由で送信されるクライアントデータを保護するために、自社のウェブサイトに適切な暗号化技術が採用されていることを確認します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	[api-gw-associated-with-waf](#)	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	netfw-policy-rule-group-associated	AWS Network Firewall ポリシーは、ファイアウォールが Amazon VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定して、パケットとトラフィックフローのフィルタリングし、デフォルトのトラフィック処理を定義します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	netfw-stateless-rule-group-not-empty	AWS Network Firewall ルールグループには、ファイアウォールが VPC 内のトラフィックを処理する方法を定義するルールが含まれています。ファイアウォールポリシーに空のステートレスルールグループが存在する場合、トラフィックは処理されません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: ファイアウォールの使用	ファイアウォールは、ネットワークに出入りするトラフィックを管理するもので、中小企業システムの保護に不可欠なツールです。ファイアウォールは、すべての重要なシステムを保護するために展開する必要がありますが、特に自社のネットワークをインターネットから保護するために、ファイアウォールを使用する必要があります。	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	elasticsearch-logs-to-cloudwatch	Amazon Elasticsearch service ドメインでエラーログが有効になっていて、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7_ネットワークのセキュリティ確保: リモートアクセスソリューションの見直し	中小企業は、リモートアクセスツールを定期的に見直して、特に以下について安全性を確認する必要があります。- すべてのリモートアクセスソフトウェアにパッチが適用され、最新であることを確認します。- 疑わしい地理的な場所や特定の IP アドレスからのリモートアクセスを制限します。- 従業員のリモートアクセスは、作業に必要なシステムとコンピュータにのみ制限します。- リモートアクセスに強力なパスワードを適用し、可能な場合は多要素認証を有効にします。- モニタリングとアラートを有効にして、疑わしい攻撃や通常とは異なる疑わしいアクティビティを警告します。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9_バックアップのセキュリティ確保	ランサムウェア攻撃などの災害からの復旧にはバックアップが有効であるため、主要な組織体制を復旧できるようにバックアップを保守管理する必要があります。次のバックアップルールを適用する必要があります。- バックアップは定期的に実行し、可能な限り自動化します。- バックアップは中小企業の本番環境とは別に保持します。- バックアップが特に拠点間で移動される場合には暗号化するようにします。- バックアップからデータを定期的にリストアする機能をテストします。理想的には、最初から最後までのフルリストアを定期的にテストする必要があります。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11_オンラインサイトのセキュリティ確保	中小企業は、オンラインウェブサイトが安全な方法で構成および維持され、クレジットカードデータなどの個人データや財務情報が適切に保護されていることを確認する必要があります。これには、ウェブサイトの潜在的なセキュリティの弱点を特定するための定期的なセキュリティテストの実施や、サイトが適切に維持および更新されていることを確認するための定期的なレビューの実施が含まれます。	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for ENISA Cyber Security guide for SMEs」で入手できます。

「Esquema Nacional de Seguridad (ENS) Low」に関する運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するよう

には設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、スペインの Esquema Nacional de Seguridad (ENS) Low フレームワークコントロールと AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールが特定の AWS リソースに適用され、1 つ以上のスペインの「ENS Low」によるコントロールに関連付けられます。スペインの「ENS」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックのサンプルテンプレートには、2020 年 10 月 23 日に最終更新されたスペインの「ENS Low」フレームワーク内のコントロールへのマッピングが含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効に

コントロール ID	AWS 設定ルール	ガイダンス
		します。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロンググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
Anexo II 4.1.2.a); b); c)	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
Anexo II 4.1.2.b)	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.b)	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
Anexo II 4.1.2.b)	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。
Anexo II 4.2.1.a)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.1.a); b)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
Anexo II 4.2.4	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.5	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.5.BAJO.a)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.5.BAJO.c)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
Anexo II 4.3.1	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.1	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
Anexo II 4.3.1	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.1	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。
Anexo II 4.3.2.b)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
Anexo II 4.3.2.b)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
Anexo II 4.3.2.b)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
Anexo II 4.3.2.b)	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
Anexo II 4.3.2.b)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
Anexo II 4.3.4.c)	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。これには、脆弱性管理ツール、環境スキャンの周期、役割と責任などが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Anexo II 4.3.8.BAJO	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
Anexo II 5.2.3	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.3.BAJO.a)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、 AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Anexo II 5.7.3	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 5.7.3	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
Anexo II 5.7.3	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
Anexo II 5.7.3	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.7.3	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Anexo II 5.7.3	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
Anexo II 5.7.3	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
Anexo II 5.8.2	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.2	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
Art. 14.4	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 16	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
Art. 16	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 16	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
Art. 20.2	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。
Art. 20.2	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。これには、脆弱性管理ツール、環境スキャンの周期、役割と責任などが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Art. 21.1	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
Art. 21.1	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Art. 21.1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
Art. 21.1	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Art. 21.1	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
Art. 21.1	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
Art. 21.1	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
Art. 21.1	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Art. 21.1	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
Art. 21.1	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Art. 21.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Art. 21.1	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
Art. 22	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
Art. 22	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
Art. 22	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Art. 22	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
Art. 22	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
Art. 22	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
Art. 22	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Art. 22	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
Art. 22	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Art. 22	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Art. 22	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
Art. 22	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
Art. 23	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
Art. 23	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Art. 23	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
Art. 23	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Art. 23	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
Art. 23	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Art. 23	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
Art. 25	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
Art. 25	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。
Art. 25	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
Art. 25	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
Art. 25	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low」で入手できます。

「Esquema Nacional de Seguridad (ENS) Medium」に関する運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下は、スペインの Esquema Nacional de Seguridad (ENS) Medium フレームワークコントロールと AWS マネージド Config ルール間のマッピングの例です。各 Config ルールは特定の AWS リソースに適用され、1 つ以上のスペインの ENS Medium コントロールに関連付けられます。スペインの

「ENS」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックのサンプルテンプレートには、2020 年 10 月 23 日に最終更新されたスペインの「ENS Medium」フレームワーク内のコントロールへのマッピングが含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があ

コントロール ID	AWS 設定ルール	ガイダンス
		るため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
Anexo II 4.1.2.a); b); c)	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
Anexo II 4.1.2.b)	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.b)	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
Anexo II 4.1.2.b)	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。
Anexo II 4.2.1.a)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.1.a); 4.2.1.b)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
Anexo II 4.2.4	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.5	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.5.a)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.5.c)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
Anexo II 4.2.6.c)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.c)	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
Anexo II 4.2.6.c)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.c)	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Anexo II 4.2.6.c)	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
Anexo II 4.2.6.c)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.c)	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Anexo II 4.2.6.c)	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.c)	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.c)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Anexo II 4.2.6.c)	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.7	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
Anexo II 4.2.7	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.7	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
Anexo II 4.2.7	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.1	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.1	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
Anexo II 4.3.1	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.1	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
Anexo II 4.3.1	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
Anexo II 4.3.2.b)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
Anexo II 4.3.2.b)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
Anexo II 4.3.2.b)	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
Anexo II 4.3.2.b)	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
Anexo II 4.3.2.b)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
Anexo II 4.3.4.c)	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。これには、脆弱性管理ツール、環境スキャンの周期、役割と責任などが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
Anexo II 4.3.7.a)	response-plan-exists-maintained (Process Check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。正式にドキュメント化された更新済みの対応計画を用意することで、対応する担当者がインシデントの発生中に従うべき役割、責任、プロセスを理解することができます。
Anexo II 4.3.8	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
Anexo II 4.3.8	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Anexo II 4.3.8	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
Anexo II 4.3.8	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Anexo II 4.3.8	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Anexo II 4.3.8	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
Anexo II 4.6.2	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.6.2	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
Anexo II 5.2.3	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
Anexo II 5.4.2	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.2	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.4.2	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.4.2	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.2	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 5.4.2	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.4.2	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.2	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
Anexo II 5.4.3	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.3	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.4.3	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.4.3	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.3	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 5.4.3	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.4.3	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.3	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.3.a)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、 AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Anexo II 5.7.3	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 5.7.3	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
Anexo II 5.7.3	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
Anexo II 5.7.3	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.7.3	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Anexo II 5.7.3	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
Anexo II 5.7.3	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
Anexo II 5.8.2	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.2	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
Anexo II 5.8.3.b)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.b)	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
Anexo II 5.8.3.b)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.b)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
Anexo II 5.8.3.b)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.b)	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.b)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.b)	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.b)	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
Art. 14.4	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 16	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
Art. 16	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 16	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
Art. 20.2	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。
Art. 20.2	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。これには、脆弱性管理ツール、環境スキャンの周期、役割と責任などが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Art. 21.1	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
Art. 21.1	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Art. 21.1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
Art. 21.1	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Art. 21.1	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
Art. 21.1	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
Art. 21.1	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
Art. 21.1	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Art. 21.1	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
Art. 21.1	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Art. 21.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Art. 21.1	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
Art. 22	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
Art. 22	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
Art. 22	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
Art. 22	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
Art. 22	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
Art. 22	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Art. 22	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
Art. 22	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Art. 22	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Art. 22	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
Art. 22	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
Art. 23	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
Art. 23	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Art. 23	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
Art. 23	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Art. 23	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
Art. 23	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Art. 23	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
Art. 24.2	response-plan-exists-maintained (Process Check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。正式にドキュメント化された更新済みの対応計画を用意することで、対応する担当者がインシデントの発生中に従うべき役割、責任、プロセスを理解することができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
Art. 25	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
Art. 25	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。
Art. 25	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
Art. 25	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
Art. 25	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium」で入手できます。

「Esquema Nacional de Seguridad (ENS) High」に関する運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下は、スペインの Esquema Nacional de Seguridad (ENS) High フレームワークコントロールと AWS マネージド Config ルール間のマッピングの例です。各 Config ルールは特定の AWS リソースに適用され、1 つ以上のスペインの ENS High コントロールに関連付けられます。スペインの

「ENS」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックのサンプルテンプレートには、2021 年 7 月 9 日に最終更新された、スペインの「ENS High」フレームワークによるコントロールへのマッピングが含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.1.ALTO	annual-risk-assessment-performed (Process check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。
4.2.1.b)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
4.2.5.ALTO.a)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代

コントロール ID	AWS 設定ルール	ガイダンス
		わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロンググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
Anexo II 4.1.2.a); b); c)	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
Anexo II 4.1.2.b)	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.b)	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
Anexo II 4.1.2.b)	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。
Anexo II 4.2.1.a)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.4	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
Anexo II 4.2.5	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.5.BAJO.a)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.5.BAJO.c)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.ALTO.b)	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
Anexo II 4.2.6.ALTO.b)	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.ALTO.b)	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
Anexo II 4.2.6.ALTO.b)	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.1	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.1	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
Anexo II 4.3.1	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.1	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
Anexo II 4.3.1	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
Anexo II 4.3.2.b)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
Anexo II 4.3.2.b)	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
Anexo II 4.3.2.b)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
Anexo II 4.3.4.c)	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。これには、脆弱性管理ツール、環境スキャンの周期、役割と責任などが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
Anexo II 4.3.7.MEDIA.a)	response-plan-exists-maintained (Process Check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。正式にドキュメント化された更新済みの対応計画を用意することで、対応する担当者がインシデントの発生中に従うべき役割、責任、プロセスを理解することができます。
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
Anexo II 4.3.8.BAJO	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Anexo II 4.3.8.BAJO	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.BAJO	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.MEDIO	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
Anexo II 4.3.8.MEDIO	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.MEDIO	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
Anexo II 4.3.8.MEDIO	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Anexo II 4.3.8.MEDIO	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.MEDIO	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
Anexo II 4.3.8.MEDIO	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Anexo II 4.3.8.MEDIO	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.MEDIO	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.8.MEDIO	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Anexo II 4.3.8.MEDIO	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.6.2.ALTO	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
Anexo II 4.6.2.MEDIA	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.2.3	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
Anexo II 5.2.4	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
Anexo II 5.2.5	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
Anexo II 5.4.2.MEDIO	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.2.MEDIO	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.4.2.MEDIO	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.4.2.MEDIO	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.2.MEDIO	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 5.4.2.MEDIO	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.2.MEDIO	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.4.2.MEDIO	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.3.BAJO.a)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.3.MEDIO	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.4.3.MEDIO	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.4.3.MEDIO	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.3.MEDIO	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.4.3.MEDIO	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 5.4.3.MEDIO	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
Anexo II 5.4.3.MEDIO	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.4.3.MEDIO	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Anexo II 5.7.3	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Anexo II 5.7.3	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
Anexo II 5.7.3	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
Anexo II 5.7.3	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Anexo II 5.7.3	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Anexo II 5.7.3	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
Anexo II 5.7.3	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.3	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
Anexo II 5.8.2	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.2	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
Anexo II 5.8.3.MEDIO.b)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.MEDIO.b)	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
Anexo II 5.8.3.MEDIO.b)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.MEDIO.b)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
Anexo II 5.8.3.MEDIO.b)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.MEDIO.b)	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.MEDIO.b)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.MEDIO.b)	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Anexo II 5.8.3.MEDIO.b)	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
Art. 14.4	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 16	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
Art. 16	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 16	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
Art. 20.2	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。
Art. 20.2	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。これには、脆弱性管理ツール、環境スキャンの周期、役割と責任などが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Art. 21.1	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
Art. 21.1	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Art. 21.1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
Art. 21.1	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Art. 21.1	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
Art. 21.1	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
Art. 21.1	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
Art. 21.1	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
Art. 21.1	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
Art. 21.1	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Art. 21.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Art. 21.1	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Art. 21.1	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 21.1	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
Art. 22	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
Art. 22	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
Art. 22	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Art. 22	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
Art. 22	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
Art. 22	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
Art. 22	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Art. 22	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。
Art. 22	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Art. 22	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Art. 22	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
Art. 22	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 22	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
Art. 23	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
Art. 23	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
Art. 23	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
Art. 23	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Art. 23	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
Art. 23	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 23	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Art. 23	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 24.2	response-plan-exists-maintained (Process Check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。正式にドキュメント化された更新済みの対応計画を用意することで、対応する担当者がインシデントの発生中に従うべき役割、責任、プロセスを理解することができます。
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
Art. 25	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
Art. 25	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。
Art. 25	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
Art. 25	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
Art. 25	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
Art. 25	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for Esquema Nacional de Seguridad (ENS) High」で入手できます。

FDA Title 21 CFR Part 11 の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、連邦規則集 (CFR) Part 11 のタイトル 21 と AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の FDA Title 21 CFR Part 11 コントロールに関連付けられます。「FDA Title 21 CFR Part 11」によるコントロー

ルを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされ	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサー

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。		ビスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.1	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれます。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10(a)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。このような手順およびコントロールには、以下が含まれるものとします。(a) 正確性、信頼性、一貫性のある意図された性能、および無効になったり変更された記録を識別する能力を確保するためのシステムの検証。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	ecr-private-lifecycle-policy-configured	Amazon Elastic Container Repository (ECR) ライフサイクルポリシーを使用すると、リポジトリ内のイメージのライフサイクル管理を有効にすることができます。これにより、未使用のイメージ (経過時間またはカウントに基づく有効期限切れイメージ) などのクリーンアップを自動化できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (c)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(c) 記録の保管期間を通して、正確かつすぐに検索できるようにするための記録の保護。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager シークレットのローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (d)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには、以下が含まれるものとします。(d) システムへのアクセスを、認可された個人に制限する。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	[api-gw-execution-logging-enabled](#)	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (e)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。こうした手順および管理には、以下が含まれます: (e) 電子記録を作成、変更、削除するオペレーターの入力やアクションの日時を個別に記録するための、安全なコンピュータで生成されたタイムスタンプ付きの監査証跡の使用。記録の変更によって、過去に記録された情報が不明瞭にならないようにするものとします。これらの監査証跡のドキュメントは、少な	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	くとも対象の電子記録に必要な期間保持され、政府機関によるレビューやコピーが可能なものとします。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (g)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(g) 認可された個人のみが、システムの使用、記録への電子署名、オペレーションシステムやコンピュータシステムへの入力または出力デバイスへのアクセス、記録の変更、手元で操作を行うことができるようにするための認証確認の使用。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (h)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(h) 必要に応じて、データ入力またはオペレーションの指示のソースの妥当性を判断するための、デバイス (例: 端末など) による確認。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (h)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(h) 必要に応じて、データ入力またはオペレーションの指示のソースの妥当性を判断するための、デバイス (例: 端末など) による確認。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (h)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(h) 必要に応じて、データ入力またはオペレーションの指示のソースの妥当性を判断するための、デバイス (例: 端末など) による確認。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (i)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。そのような手順および統制には、以下が含まれます。(i) 電子記録/電子署名システムを開発、維持、または使用する者が、割り当てられたタスクを実行するための教育、訓練、および経験を有するかどうかの判断。	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.10 (k)	電子記録を作成、修正、維持、または送信するためのクローズドシステムを使用する人物は、電子記録の真正性、完全性、さらに必要に応じて機密性を確保し、署名者によって、署名された記録が正規のものではないという否認を容易にされないようにするために設計された手順と管理を採用するものとします。これらの手順とコントロールには以下が含まれるものとします。(k) 以下を含む、システムドキュメントに関する適切なコントロールの使用。(1) システム運用および保守のためのドキュメントの配布、アクセス、使用に対する適切なコントロール。(2) システムドキュメントの開発と変更を時系列で記録する監査証跡を維持するための改訂および変更管理手順。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	(a) 生体認証に基づかない電子署名では、以下を行うものとします。(1) 識別コードやパスワードなど、少なくとも 2 つの異なる識別コンポーネントを使用する。(i) 個人が、制御された単一のシステムへの連続したアクセス期間中に一連の署名を実行する場合、最初の署名はすべての電子署名コンポーネントを使用して実行されなければならず、後続の署名は、個人によってのみ実行可能であり、個人によってのみ使用されるよう設計された少なくとも 1 つの電子署名コンポーネントを使用して実行される。(ii) 個人が、継続的に制御された単一のシステムへのアクセス期間中に実行されなかった 1 つ以上の署名を実行する場合、各署名は、すべての電子署名コンポーネントを使用し	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	て実行される。(2) 正規の所有者のみが使用する。(3) 正規の所有者以外が個人の電子署名の使用を試みた場合は、2 人以上の個人による協力を必要とするようにコントロールし実行する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	(a) 生体認証に基づかない電子署名では、以下を行うものとします。(1) 識別コードやパスワードなど、少なくとも 2 つの異なる識別コンポーネントを使用する。(i) 個人が、制御された単一のシステムへの連続したアクセス期間中に一連の署名を実行する場合、最初の署名はすべての電子署名コンポーネントを使用して実行されなければならず、後続の署名は、個人によってのみ実行可能であり、個人によってのみ使用されるよう設計された少なくとも 1 つの電子署名コンポーネントを使用して実行される。(ii) 個人が、継続的に制御された単一のシステムへのアクセス期間中に実行されなかった 1 つ以上の署名を実行する場合、各署名は、すべての電子署名コンポーネントを使用し	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	て実行される。(2) 正規の所有者のみが使用する。(3) 正規の所有者以外が個人の電子署名の使用を試みた場合は、2 人以上の個人による協力を必要とするようにコントロールし実行する。		のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	(a) 生体認証に基づかない電子署名では、以下を行うものとします。(1) 識別コードやパスワードなど、少なくとも 2 つの異なる識別コンポーネントを使用する。(i) 個人が、制御された単一のシステムへの連続したアクセス期間中に一連の署名を実行する場合、最初の署名はすべての電子署名コンポーネントを使用して実行されなければならず、後続の署名は、個人によってのみ実行可能であり、個人によってのみ使用されるよう設計された少なくとも 1 つの電子署名コンポーネントを使用して実行される。(ii) 個人が、継続的に制御された単一のシステムへのアクセス期間中に実行されなかった 1 つ以上の署名を実行する場合、各署名は、すべての電子署名コンポーネントを使用し	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	て実行される。(2) 正規の所有者のみが使用する。(3) 正規の所有者以外が個人の電子署名の使用を試みた場合は、2 人以上の個人による協力を必要とするようにコントロールし実行する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	(a) 生体認証に基づかない電子署名では、以下を行うものとします。(1) 識別コードやパスワードなど、少なくとも 2 つの異なる識別コンポーネントを使用する。(i) 個人が、制御された単一のシステムへの連続したアクセス期間中に一連の署名を実行する場合、最初の署名はすべての電子署名コンポーネントを使用して実行されなければならず、後続の署名は、個人によってのみ実行可能であり、個人によってのみ使用されるよう設計された少なくとも 1 つの電子署名コンポーネントを使用して実行される。(ii) 個人が、継続的に制御された単一のシステムへのアクセス期間中に実行されなかった 1 つ以上の署名を実行する場合、各署名は、すべての電子署名コンポーネントを使用し	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	て実行される。(2) 正規の所有者のみが使用する。(3) 正規の所有者以外が個人の電子署名の使用を試みた場合は、2 人以上の個人による協力を必要とするようにコントロールし実行する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	(a) 生体認証に基づかない電子署名では、以下を行うものとします。(1) 識別コードやパスワードなど、少なくとも 2 つの異なる識別コンポーネントを使用する。(i) 個人が、制御された単一のシステムへの連続したアクセス期間中に一連の署名を実行する場合、最初の署名はすべての電子署名コンポーネントを使用して実行されなければならず、後続の署名は、個人によってのみ実行可能であり、個人によってのみ使用されるよう設計された少なくとも 1 つの電子署名コンポーネントを使用して実行される。(ii) 個人が、継続的に制御された単一のシステムへのアクセス期間中に実行されなかった 1 つ以上の署名を実行する場合、各署名は、すべての電子署名コンポーネントを使用し	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	て実行される。(2) 正規の所有者のみが使用する。(3) 正規の所有者以外が個人の電子署名の使用を試みた場合は、2 人以上の個人による協力を必要とするようにコントロールし実行する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	(a) 生体認証に基づかない電子署名では、以下を行うものとします。(1) 識別コードやパスワードなど、少なくとも 2 つの異なる識別コンポーネントを使用する。(i) 個人が、制御された単一のシステムへの連続したアクセス期間中に一連の署名を実行する場合、最初の署名はすべての電子署名コンポーネントを使用して実行されなければならず、後続の署名は、個人によってのみ実行可能であり、個人によってのみ使用されるよう設計された少なくとも 1 つの電子署名コンポーネントを使用して実行される。(ii) 個人が、継続的に制御された単一のシステムへのアクセス期間中に実行されなかった 1 つ以上の署名を実行する場合、各署名は、すべての電子署名コンポーネントを使用し	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	て実行される。(2) 正規の所有者のみが使用する。(3) 正規の所有者以外が個人の電子署名の使用を試みた場合は、2 人以上の個人による協力を必要とするようにコントロールし実行する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.2	(a) 生体認証に基づかない電子署名では、以下を行うものとします。(1) 識別コードやパスワードなど、少なくとも 2 つの異なる識別コンポーネントを使用する。(i) 個人が、制御された単一のシステムへの連続したアクセス期間中に一連の署名を実行する場合、最初の署名はすべての電子署名コンポーネントを使用して実行されなければならず、後続の署名は、個人によってのみ実行可能であり、個人によってのみ使用されるよう設計された少なくとも 1 つの電子署名コンポーネントを使用して実行される。(ii) 個人が、継続的に制御された単一のシステムへのアクセス期間中に実行されなかった 1 つ以上の署名を実行する場合、各署名は、すべての電子署名コンポーネントを使用し	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	て実行される。(2) 正規の所有者のみが使用する。(3) 正規の所有者以外が個人の電子署名の使用を試みた場合は、2 人以上の個人による協力を必要とするようにコントロールし実行する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.3	オープンシステムを使用して電子記録を作成、修正、維持、送信する人物は、電子記録の作成時点から受領時点まで、電子記録の真正性、完全性、さらに必要に応じて機密性を確保するために設計された手順とコントロールを採用するものとします。このような手順とコントロールには、11.10 の指定によるもののほか、必要に応じて記録の真正性、完全性、機密性を確保するためのドキュメントの暗号化や、適切なデジタル署名の規格の使用などの追加措置が含まれるものとします。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (b)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(b) 識別コードおよびパスワードの発行が定期的にチェック、リコールされ、改訂されていることを確認する (例: 古いパスワードなどに対応するため)。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (b)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(b) 識別コードおよびパスワードの発行が定期的にチェック、リコールされ、改訂されていることを確認する (例: 古いパスワードなどに対応するため)。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (b)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(b) 識別コードおよびパスワードの発行が定期的にチェック、リコールされ、改訂されていることを確認する (例: 古いパスワードなどに対応するため)。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (b)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(b) 識別コードおよびパスワードの発行が定期的にチェック、リコールされ、改訂されていることを確認する (例: 古いパスワードなどに対応するため)。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (b)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(b) 識別コードおよびパスワードの発行が定期的にチェック、リコールされ、改訂されていることを確認する (例: 古いパスワードなどに対応するため)。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (b)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(b) 識別コードおよびパスワードの発行が定期的にチェック、リコールされ、改訂されていることを確認する (例: 古いパスワードなどに対応するため)。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (d)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(d) パスワードおよび/または識別コードの不正使用を防止するためのトランザクションのセーフガードの使用、ならびにシステムセキュリティユニットの不正使用の試みを検知し、必要に応じて組織の管理者に即時かつ緊急に報告する。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (d)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(d) パスワードおよび/または識別コードの不正使用を防止するためのトランザクションのセーフガードの使用、ならびにシステムセキュリティユニットの不正使用の試みを検知し、必要に応じて組織の管理者に即時かつ緊急に報告する。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (d)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(d) パスワードおよび/または識別コードの不正使用を防止するためのトランザクションのセーフガードの使用、ならびにシステムセキュリティユニットの不正使用の試みを検知し、必要に応じて組織の管理者に即時かつ緊急に報告する。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.300 (d)	識別コードとパスワードを組み合わせた電子署名を使用する人物は、その安全性と完全性を確保するためのコントロールを行うものとします。これらのコントロールには以下が含まれるものとします。(d) パスワードおよび/または識別コードの不正使用を防止するためのトランザクションのセーフガードの使用、ならびにシステムセキュリティユニットの不正使用の試みを検知し、必要に応じて組織の管理者に即時かつ緊急に報告する。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for FDA Title 21 CFR Part 11」で入手できます。

FedRAMP (Low) の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレート

としてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Federal Risk and Authorization Management Program (FedRAMP) Low Baseline Controls と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の FedRAMP コントロールに関連付けられます。「FedRAMP」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
AC-2	アカウントの管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			たアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-2	アカウントの管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AC-2	アカウントの管理	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-2	アカウントの管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-2	アカウントの管理	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウントの管理	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
AC-3	アクセスの実施	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-3	アクセスの実施	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
AC-3	アクセスの実施	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-3	アクセスの実施	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-3	アクセスの実施	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-3	アクセスの実施	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-3	アクセスの実施	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-3	アクセスの実施	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-3	アクセスの実施	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
AC-17	リモートアクセス	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-17	リモートアクセス	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-17	リモートアクセス	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-17	リモートアクセス	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-17	リモートアクセス	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-17	リモートアクセス	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-17	リモートアクセス	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17	リモートアクセス	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	監査イベント	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	監査イベント	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	監査イベント	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	監査イベント	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-2	監査イベント	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	監査イベント	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-2	監査イベント	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	監査イベント	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-2	監査イベント	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	監査イベント	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	監査イベント	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	監査イベント	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-3	監査記録の内容	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-3	監査記録の内容	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-3	監査記録の内容	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-3	監査記録の内容	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-6	監査レビュー、分析、および報告	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-6	監査レビュー、分析、および報告	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-6	監査レビュー、分析、および報告	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AU-6	監査レビュー、分析、および報告	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6	監査レビュー、分析、および報告	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-9	監査情報の保護	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9	監査情報の保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
AU-9	監査情報の保護	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9	監査情報の保護	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
AU-9	監査情報の保護	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-11	監査記録の保持	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
AU-12	監査世代	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査世代	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査世代	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査世代	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-12	監査世代	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査世代	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-12	監査世代	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査世代	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-12	監査世代	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査世代	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査世代	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査世代	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
CA-7	継続的なモニタリング	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
CA-7	継続的なモニタリング	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CA-7	継続的なモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
CA-7	継続的なモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
CM-2	ベースラインの設定	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CM-2	ベースラインの設定	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
CM-2	ベースラインの設定	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CM-2	ベースラインの設定	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CM-2	ベースラインの設定	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
CM-2	ベースラインの設定	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
CM-2	ベースラインの設定	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
CM-7	最小の機能	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-7	最小の機能	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-7	最小の機能	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8	情報システムのコンポーネントのインベントリ	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8	情報システムのコンポーネントのインベントリ	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8	情報システムのコンポーネントのインベントリ	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CM-8	情報システムのコンポーネントのインベントリ	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
CP-9	情報システムのバックアップ	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	バックアップ計画によって保護されたEBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-9	情報システムのバックアップ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システムのバックアップ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
CP-10	情報システムの復旧と再構築	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
CP-10	情報システムの復旧と再構築	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-10	情報システムの復旧と再構築	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CP-10	情報システムの復旧と再構築	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	情報システムの復旧と再構築	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2	身分証明書と認証 (組織のユーザー)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA-2	身分証明書と認証 (組織のユーザー)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2	身分証明書と認証 (組織のユーザー)	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2	身分証明書と認証 (組織のユーザー)	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2	身分証明書と認証 (組織のユーザー)	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2	身分証明書と認証 (組織のユーザー)	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5	Authenticator の管理	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5	Authenticator の管理	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4	インシデントハンドリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4	インシデントハンドリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4	インシデントハンドリング	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4	インシデントハンドリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4	インシデントハンドリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-6	インシデントの報告	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-6	インシデントの報告	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-6	インシデントの報告	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-7	インシデント対応の改善	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-7	インシデント対応の改善	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-7	インシデント対応の改善	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5	脆弱性スキャン	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5	脆弱性スキャン	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5	脆弱性スキャン	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3	システム開発のライフサイクル	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3	システム開発のライフサイクル	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3	システム開発のライフサイクル	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
SC-5	サービス拒否からの保護	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
SC-5	サービス拒否からの保護	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
SC-5	サービス拒否からの保護	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
SC-5	サービス拒否からの保護	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
SC-7	境界保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
SC-7	境界保護	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-7	境界保護	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7	境界保護	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7	境界保護	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-7	境界保護	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。
SC-12	暗号化キーの確立と管理	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12	暗号化キーの確立と管理	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12	暗号化キーの確立と管理	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
SC-13	暗号化による保護	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
SC-13	暗号化による保護	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-13	暗号化による保護	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
SI-2	欠陥修復	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3	欠陥修復	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3	欠陥修復	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
SI-3	欠陥修復	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service (Amazon ECS) コンテナで使用できる最大メモリを制限することで、コンテナへの悪意のあるアクセスが発生しても、リソースの使用量が悪用されることはありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
SI-4	情報システムのモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
SI-4	情報システムのモニタリング	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
SI-4	情報システムのモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	情報システムのモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	セキュリティアラート、勧告、および指示	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	セキュリティアラート、勧告、および指示	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	セキュリティアラート、勧告、および指示	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	セキュリティアラート、勧告、および指示	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
SI-12	情報の取り扱いと保持	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の取り扱いと保持	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
SI-16	メモリ保護	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service (Amazon ECS) コンテナで使用できる最大メモリを制限することで、コンテナへの悪意のあるアクセスが発生しても、リソースの使用量が悪用されることはありません。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for FedRAMP (Low)」で入手できます。

FedRAMP(Moderate) に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Federal Risk and Authorization Management Program (FedRAMP) と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の FedRAMP コントロールに関連付けられます。「FedRAMP」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックは、Payment Card Industry Qualified Security Assessors (QSAs)、HITRUST Certified Common Security Framework Practitioners (CCSFPs)、およびさまざまな業界フレームワークのガイダンスと評価を提供することを認定されたコンプライアンスプロフェッショナルのチームである AWS Security Assurance Services LLC (AWS SAS) によって検証されました。 AWS SAS プロフェッショナルは、お客様が FedRAMP コントロールのサブセットに合わせることができるようにこのコンフォーマンスパックを設計しました。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (3)	情報システムは、ユーザーの非アクティブな状態が 90 日を経過すると、自動的にアカウントを無効にします。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (3)	情報システムは、ユーザーの非アクティブな状態が 90 日を経過すると、自動的にアカウントを無効にします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員または役割)] に通知します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (12)(a)	組織: a。[Assignment: organization-defined atypical use (割り当て: 組織で定義された非定型の使用)] の情報システムアカウントをモニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (12)(a)	組織: a。[Assignment: organization-defined atypical use (割り当て: 組織で定義された非定型の使用)] の情報システムアカウントをモニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
AC-6 (10)	情報システムは、非特権ユーザーが特権的機能を実行して、実装されたセキュリティの保護/対策を無効化、回避、変更することを防ぎます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 (10)	情報システムは、非特権ユーザーが特権的機能を実行して、実装されたセキュリティの保護/対策を無効化、回避、変更することを防ぎます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 (10)	情報システムは、非特権ユーザーが特権的機能を実行して、実装されたセキュリティの保護/対策を無効化、回避、変更することを防ぎます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	[api-gw-execution-logging-enabled](#)	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-7 (1)	情報システムは、[Assignment: organization-defined audit fields within audit records (割り当て: 組織で定義された監査レコード内の監査フィールド)] に基づいて、対象のイベントの監査レコードを処理する機能を提供します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-7 (1)	情報システムは、[Assignment: organization-defined audit fields within audit records (割り当て: 組織で定義された監査レコード内の監査フィールド)] に基づいて、対象のイベントの監査レコードを処理する機能を提供します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9 (2)	情報システムは、少なくとも週に一度、監査記録を監査対象のシステムやコンポーネントとは物理的に異なるシステムまたはシステムコンポーネントにバックアップします。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9 (2)	情報システムは、少なくとも週に一度、監査記録を監査対象のシステムやコンポーネントとは物理的に異なるシステムまたはシステムコンポーネントにバックアップします。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
AU-9	情報システムは、監査情報と監査ツールを不正アクセス、変更、削除から保護します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9	情報システムは、監査情報と監査ツールを不正アクセス、変更、削除から保護します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
AU-9	情報システムは、監査情報と監査ツールを不正アクセス、変更、削除から保護します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-11	組織は、セキュリティインシデントの事後調査を支援するため、また、規制および組織の情報保持要件を満たすために、監査レコードを少なくとも 90 日間保持します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
CM-7 (a)	組織: a。重要な機能のみを提供するように情報システムを設定します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-7 (a)	組織: a。重要な機能のみを提供するように情報システムを設定します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-7 (a)	組織: a。重要な機能のみを提供するように情報システムを設定します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (1)	組織は、コンポーネントのインストール、削除、および情報システムの更新において不可欠な部分である情報システムコンポーネントのインベントリを更新します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (1)	組織は、コンポーネントのインストール、削除、および情報システムの更新において不可欠な部分である情報システムコンポーネントのインベントリを更新します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (3)(a)	組織: a。情報システム内に存在する未承認のハードウェア、ソフトウェア、ファームウェアのコンポーネントを検出するため、検出に最大 5 分の遅延をともなう自動化されたメカニズムを継続的に使用します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (3)(a)	組織: a。情報システム内に存在する未承認のハードウェア、ソフトウェア、ファームウェアのコンポーネントを検出するため、検出に最大 5 分の遅延をともなう自動化されたメカニズムを継続的に使用します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (3)(a)	組織: a。情報システム内に存在する未承認のハードウェア、ソフトウェア、ファームウェアのコンポーネントを検出するため、検出に最大 5 分の遅延をともなう自動化されたメカニズムを継続的に使用します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CM-8 (3)(a)	組織: a。情報システム内に存在する未承認のハードウェア、ソフトウェア、ファームウェアのコンポーネントを検出するため、検出に最大 5 分の遅延をともなう自動化されたメカニズムを継続的に使用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)(2)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(2) 情報システムは、非特権アカウントへのネットワークアクセスのための多要素認証を実装します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)(2)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(2) 情報システムは、非特権アカウントへのネットワークアクセスのための多要素認証を実装します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)(2)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(2) 情報システムは、非特権アカウントへのネットワークアクセスのための多要素認証を実装します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)(2)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(2) 情報システムは、非特権アカウントへのネットワークアクセスのための多要素認証を実装します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2	情報システムは、組織のユーザー (または組織のユーザーに代わって実行するプロセス) を一意に識別し認証します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA-2	情報システムは、組織のユーザー (または組織のユーザーに代わって実行するプロセス) を一意に識別し認証します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5 (1)(a)(d)(e)	パスワードベースの認証のための情報システム: a。[Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type (割り当て: 組織で定義された大文字と小文字の区別、文字数、大文字、小文字、数字、特殊文字の組み合わせに関する、各タイプの最小要件を含む要件)] のパスワードの複雑さを最小限に抑えます: d。[Assignment: organization- defined numbers for lifetime minimum, lifetime maximum (割り当て: 組織で定義されたライフタイムの最小および最大の数値)] のパスワードの最小および最大有効期間の制限を適用します:	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	e。24 世代にわたるパスワードの再利用の禁止		のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5 (4)	組織は、自動化されたツールを使用して、パスワード認証システムに [Assignment: organization-defined requirements (割り当て: 組織で定義された要件)] を満たす十分な強度があるかどうかを判断します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA-5 (7)	組織は、暗号化されていない静的オーセンティケーターが、アプリケーションやアクセススクリプトに埋め込まれたり、ファンクションキーに割り当てられたりしていないことを確認します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-6 (1)	組織は、セキュリティインシデントの報告をサポートするための自動化されたメカニズムを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-6 (1)	組織は、セキュリティインシデントの報告をサポートするための自動化されたメカニズムを採用します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-6 (1)	組織は、セキュリティインシデントの報告をサポートするための自動化されたメカニズムを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-7 (1)	組織は、インシデント対応に関連する情報およびサポートの可用性を高めるための自動化されたメカニズムを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-7 (1)	組織は、インシデント対応に関連する情報およびサポートの可用性を高めるための自動化されたメカニズムを採用します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-7 (1)	組織は、インシデント対応に関連する情報およびサポートの可用性を高めるための自動化されたメカニズムを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5(1)	組織は、スキャン対象の情報システムの脆弱性を簡単に更新できる機能を含む脆弱性スキャンツールを採用しています。補足ガイダンス: 新しい脆弱性が発見され、発表され、スキャン方法が開発されたときは、スキャン対象の脆弱性をすぐに更新する必要があります。この更新プロセスにより、情報システムの潜在的な脆弱性が可能な限り迅速に特定され、対処されます。関連コントロール: SI-3、SI-7。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5(1)	組織は、スキャン対象の情報システムの脆弱性を簡単に更新できる機能を含む脆弱性スキャンツールを採用しています。補足ガイダンス: 新しい脆弱性が発見され、発表され、スキャン方法が開発されたときは、スキャン対象の脆弱性をすぐに更新する必要があります。この更新プロセスにより、情報システムの潜在的な脆弱性が可能な限り迅速に特定され、対処されます。関連コントロール: SI-3、SI-7。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5(1)	組織は、スキャン対象の情報システムの脆弱性を簡単に更新できる機能を含む脆弱性スキャンツールを採用しています。補足ガイダンス: 新しい脆弱性が発見され、発表され、スキャン方法が開発されたときは、スキャン対象の脆弱性をすぐに更新する必要があります。この更新プロセスにより、情報システムの潜在的な脆弱性が可能な限り迅速に特定され、対処されます。関連コントロール: SI-3、SI-7。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5	組織: a。情報システムおよびホストされているアプリケーションの脆弱性を毎月スキャンし [operating system/infrastructure; monthly web applications and databases (オペレーティングシステム/インフラストラクチャ、毎月のウェブアプリケーションおよびデータベース)]、システム/アプリケーションに影響を与える可能性のある新たな脆弱性が特定され、報告された場合にもスキャンします: b。ツール間の相互運用性を促進し、脆弱性管理プロセスの一部を自動化するために、以下の標準を使用した脆弱性スキャンツールおよびテクノロジーを採用します: 1。プラットフォーム、ソフトウェアの欠陥、不適切な構成を列挙します: 2。チェックリストとテスト手順	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	のフォーマット: および 3。脆弱性による影響の測定: c。脆弱性スキャンレポートとセキュリティコントロール評価の結果を分析します: d。正当性のある脆弱性の修正: 組織のリスク評価に基づき、発見日から (30) 日以内に緩和された高リスクの脆弱性、発見日から (90) 日以内に緩和された中程度のリスクの脆弱性、発見日から (180) 日以内に緩和された低リスクの脆弱性: および e。脆弱性スキャンプロセスおよびセキュリティコントロール評価から取得した情報を [Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] と共有し、他の情報システムにおける同様の脆弱性 (システム的な弱点や欠陥) を排除します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5	組織: a。情報システムおよびホストされているアプリケーションの脆弱性をスキャンし [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process (割り当て: 組織で定義された頻度および/またはプロセスに従ったランダムな頻度)]、システム/アプリケーションに影響を与える可能性のある新たな脆弱性が特定され、報告された場合にもスキャンします: b。ツール間の相互運用性を促進し、脆弱性管理プロセスの一部を自動化するために、以下の標準を使用した脆弱性スキャンツールおよびテクノロジーを採用します: 1。プラットフォーム、ソフトウェアの欠陥、不適切な構成を列挙します: 2。チェックリストとテスト手順	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	のフォーマット: および 3。脆弱性による影響の測定: c。脆弱性スキャンレポートとセキュリティコントロール評価の結果を分析します: d。リスクの組織的評価に従って、正当な脆弱性を修正します: [Assignment: organization-defined response times (割り当て: 組織で定義された応答時間)]: および e。脆弱性スキャンプロセスおよびセキュリティコントロール評価から取得した情報を [Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] と共有し、他の情報システムにおける同様の脆弱性 (システム的な弱点や欠陥) を排除します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3 (a)	組織: a。情報セキュリティの考慮事項が組み込まれた [Assignment: organization-defined system development life cycle (割り当て: 組織で定義されたシステム開発のライフサイクル)] を使用して、情報システムを管理します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3 (a)	組織: a。情報セキュリティの考慮事項が組み込まれた [Assignment: organization-defined system development life cycle (割り当て: 組織で定義されたシステム開発のライフサイクル)] を使用して、情報システムを管理します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3 (a)	組織: a。情報セキュリティの考慮事項が組み込まれた [Assignment: organization-defined system development life cycle (割り当て: 組織で定義されたシステム開発のライフサイクル)] を使用して、情報システムを管理します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、サービスの開発および実装と運用の際に設定管理を行う: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響をドキュメント化する: および e。システム、コンポーネン	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ト、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、サービスの開発および実装と運用の際に設定管理を行う: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響をドキュメント化する: および e。システム、コンポーネン	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ト、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、サービスの開発および実装と運用の際に設定管理を行う: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響をドキュメント化する: および e。システム、コンポーネン	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ト、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、サービスの開発および実装と運用の際に設定管理を行う: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響をドキュメント化する: および e。システム、コンポーネン	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ト、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(5)	マネージドインターフェイスの情報システムは、デフォルトでネットワーク通信トラフィックを拒否し、例外的にネットワーク通信トラフィックを許可します (つまりすべてを拒否し、例外的に許可)。補足ガイダンス: この制御の強化は、インバウンドネットワーク通信トラフィックとアウトバウンドネットワーク通信トラフィックの両方に適用されます。deny-all (すべて拒否)、permit-by-exception (例外による許可) のネットワーク通信トラフィックポリシーでは、必須かつ承認された接続のみが許可されます。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12	組織は、[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] に従って、情報システム内で使用される必要な暗号化の暗号化キーを確立および管理します。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。
SC-12	組織は、[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] に従って、情報システム内で使用される必要な暗号化の暗号化キーを確立および管理します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12	組織は、[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] に従って、情報システム内で使用される必要な暗号化の暗号化キーを確立および管理します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-23	情報システムは、通信セッションの信頼性を保護します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	情報システムは、通信セッションの信頼性を保護します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23	情報システムは、通信セッションの信頼性を保護します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23	情報システムは、通信セッションの信頼性を保護します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	情報システムは、通信セッションの信頼性を保護します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23	情報システムは、通信セッションの信頼性を保護します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2 (2)	組織は、欠陥の修復に関する情報システムのコンポーネントの状態を判断するため、少なくとも月に一度、自動化されたメカニズムを採用します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2 (2)	組織は、欠陥の修復に関する情報システムのコンポーネントの状態を判断するため、少なくとも月に一度、自動化されたメカニズムを採用します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2 (2)	組織は、欠陥の修復に関する情報システムのコンポーネントの状態を判断するため、少なくとも月に一度、自動化されたメカニズムを採用します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
SI-2 (2)	組織は、欠陥の修復に関する情報システムのコンポーネントの状態を判断するため、少なくとも月に一度、自動化されたメカニズムを採用します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3	組織: a。情報システムの入口と出口に悪意のあるコードに対する保護メカニズムを採用して、悪意のあるコードを検出して根絶します。b。組織の構成管理ポリシーと手順に従って、新しいリリースが公開されるたびに、悪意のあるコードに対する保護メカニズムを更新します。c。悪意あるコードの保護機構を 1 に設定します。組織のセキュリティポリシーに従ってファイルがダウンロード、開く、または実行されるときに、情報システム [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] を定期的にスキャンし、[Selection(one or more); endpoint; network entry/exit points (選択 (1 つ以上)、エンドポイント、ネットワークの入口/出	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ロポイント)] で外部ソースからのファイルのリアルタイムスキャンを実行します。2. 悪意のあるコードが検出されると、[Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action] (選択 (1 つ以上): 悪意のあるコードのブロック、悪意のあるコードの隔離、管理者にアラートを送信)、割り当て:組織であるコードのブロが行われます。悪意のあるコードの検出および根絶中に受信する誤検出、およびその結果生じる情報システムの可用性への潜在的な影響に対処します。補足ガイダンス: 情報システムの入口と出口には、ファイアウォール、電子メールサーバー、ウェブサーバー、プロキシサーバー、リモー		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	トアクセスサーバー、ワークステーション、ノートパソコン、モバイルデバイスなどが含まれます。悪意のあるコードには、ウイルス、ワーム、トロイの木馬、スパイウェアなどが含まれます。悪意のあるコードは、さまざまな形式 (例: UUENCODE、Unicode) でエンコードされたり、圧縮されたファイルや隠しファイルに格納されたり、またはステガノグラフィを使用してファイルに隠されたりすることもあります。悪意のあるコードは、ウェブアクセス、電子メール、電子メールの添付ファイル、ポータブルストレージデバイスなど、さまざまな方法で転送される可能性があります。悪意のあるコードの挿入は、情報システムの脆弱性を悪用することによって行われます。悪意		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	のあるコードに対する保護メカニズムには、たとえば、ウイルス対策シグネチャの定義やレピュテーションベースの技術が含まれます。悪意のあるコードの影響を制限または排除するためのさまざまな技術や方法が存在します。広範囲にわたる構成管理と包括的なソフトウェアの整合性の制御は、不正なコードの実行を防止するのに効果的な場合があります。市販のソフトウェアに加えて、カスタムビルドのソフトウェアにも悪意のあるコードが含まれている可能性があります。これには、ロジックボム、バックドア、および組織のミッション/ビジネス機能に影響を与える可能性のあるその他のタイプのサイバー攻撃などが含まれます。従来の悪意のあるコードに対する保護メカニズムでは、このよ		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	うなコードを常に検出できるとは限りません。このような状況では、組織は代わりに、ソフトウェアが意図した機能以外を実行しないようにするために、安全なコーディング手法、構成の管理と制御、信頼できる調達プロセス、監視方法などの他の保護手段を使用しています。組織は、悪意のあるコードの検出に対応するため、さまざまなアクションが必要であると判断する場合があります。例えば、組織は、定期的なスキャン中の悪意のあるコードの検出に対応するアクション、悪意のあるダウンロードの検出に対応するアクション、および/またはファイルを開いたり実行しようとしたときの悪意のある検出に対応するアクションを定義できます。関連コントロール: CM-3、MP-2、SA-4、SA-		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	8、SA-12、SA-13、SC-7、SC-26、SC-44、SI-2、SI-4、SI-7。参考文献: NIST 特別刊行物 800-83。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3	組織: a。情報システムの入口と出口に悪意のあるコードに対する保護メカニズムを採用して、悪意のあるコードを検出して根絶します。b。組織の構成管理ポリシーと手順に従って、新しいリリースが公開されるたびに、悪意のあるコードに対する保護メカニズムを更新します。c。悪意あるコードの保護機構を 1 に設定します。組織のセキュリティポリシーに従ってファイルがダウンロード、開く、または実行されるときに、情報システム [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] を定期的にスキャンし、[Selection(one or more); endpoint; network entry/exit points (選択 (1 つ以上)、エンドポイント、ネットワークの入口/出	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ロポイント)] で外部ソースからのファイルのリアルタイムスキャンを実行します。2. 悪意のあるコードが検出されると、[Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action] (選択 (1 つ以上): 悪意のあるコードのブロック、悪意のあるコードの隔離、管理者にアラートを送信)、割り当て:組織であるコードのブロが行われます。悪意のあるコードの検出および根絶中に受信する誤検出、およびその結果生じる情報システムの可用性への潜在的な影響に対処します。補足ガイダンス: 情報システムの入口と出口には、ファイアウォール、電子メールサーバー、ウェブサーバー、プロキシサーバー、リモー		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	トアクセスサーバー、ワークステーション、ノートパソコン、モバイルデバイスなどが含まれます。悪意のあるコードには、ウイルス、ワーム、トロイの木馬、スパイウェアなどが含まれます。悪意のあるコードは、さまざまな形式 (例: UUENCODE、Unicode) でエンコードされたり、圧縮されたファイルや隠しファイルに格納されたり、またはステガノグラフィを使用してファイルに隠されたりすることもあります。悪意のあるコードは、ウェブアクセス、電子メール、電子メールの添付ファイル、ポータブルストレージデバイスなど、さまざまな方法で転送される可能性があります。悪意のあるコードの挿入は、情報システムの脆弱性を悪用することによって行われます。悪意		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	のあるコードに対する保護メカニズムには、たとえば、ウイルス対策シグネチャの定義やレピュテーションベースの技術が含まれます。悪意のあるコードの影響を制限または排除するためのさまざまな技術や方法が存在します。広範囲にわたる構成管理と包括的なソフトウェアの整合性の制御は、不正なコードの実行を防止するのに効果的な場合があります。市販のソフトウェアに加えて、カスタムビルドのソフトウェアにも悪意のあるコードが含まれている可能性があります。これには、ロジックボム、バックドア、および組織のミッション/ビジネス機能に影響を与える可能性のあるその他のタイプのサイバー攻撃などが含まれます。従来の悪意のあるコードに対する保護メカニズムでは、このよ		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	うなコードを常に検出できるとは限りません。このような状況では、組織は代わりに、ソフトウェアが意図した機能以外を実行しないようにするために、安全なコーディング手法、構成の管理と制御、信頼できる調達プロセス、監視方法などの他の保護手段を使用しています。組織は、悪意のあるコードの検出に対応するため、さまざまなアクションが必要であると判断する場合があります。例えば、組織は、定期的なスキャン中の悪意のあるコードの検出に対応するアクション、悪意のあるダウンロードの検出に対応するアクション、および/またはファイルを開いたり実行しようとしたときの悪意のある検出に対応するアクションを定義できます。関連コントロール: CM-3、MP-2、SA-4、SA-		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	8、SA-12、S A-13、SC-7 、SC-26、SC -44、SI-2、SI-4、SI-7 。参考文献: NIST 特 別刊行物 800-83。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3	組織: a。情報システムの入口と出口に悪意のあるコードに対する保護メカニズムを採用して、悪意のあるコードを検出して根絶します。b。組織の構成管理ポリシーと手順に従って、新しいリリースが公開されるたびに、悪意のあるコードに対する保護メカニズムを更新します。c。悪意あるコードの保護機構を 1 に設定します。組織のセキュリティポリシーに従ってファイルがダウンロード、開く、または実行されるときに、情報システム [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] を定期的にスキャンし、[Selection(one or more); endpoint; network entry/exit points (選択 (1 つ以上)、エンドポイント、ネットワークの入口/出	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service (Amazon ECS) コンテナで使用できる最大メモリを制限することで、コンテナへの悪意のあるアクセスが発生しても、リソースの使用量が悪用されることはありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ロポイント)] で外部ソースからのファイルのリアルタイムスキャンを実行します。2. 悪意のあるコードが検出されると、[Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action] (選択 (1 つ以上): 悪意のあるコードのブロック、悪意のあるコードの隔離、管理者にアラートを送信)、割り当て:組織であるコードのブロが行われます。悪意のあるコードの検出および根絶中に受信する誤検出、およびその結果生じる情報システムの可用性への潜在的な影響に対処します。補足ガイダンス: 情報システムの入口と出口には、ファイアウォール、電子メールサーバー、ウェブサーバー、プロキシサーバー、リモー		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	トアクセスサーバー、ワークステーション、ノートパソコン、モバイルデバイスなどが含まれます。悪意のあるコードには、ウイルス、ワーム、トロイの木馬、スパイウェアなどが含まれます。悪意のあるコードは、さまざまな形式 (例: UUENCODE、Unicode) でエンコードされたり、圧縮されたファイルや隠しファイルに格納されたり、またはステガノグラフィを使用してファイルに隠されたりすることもあります。悪意のあるコードは、ウェブアクセス、電子メール、電子メールの添付ファイル、ポータブルストレージデバイスなど、さまざまな方法で転送される可能性があります。悪意のあるコードの挿入は、情報システムの脆弱性を悪用することによって行われます。悪意		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	のあるコードに対する保護メカニズムには、たとえば、ウイルス対策シグネチャの定義やレピュテーションベースの技術が含まれます。悪意のあるコードの影響を制限または排除するためのさまざまな技術や方法が存在します。広範囲にわたる構成管理と包括的なソフトウェアの整合性の制御は、不正なコードの実行を防止するのに効果的な場合があります。市販のソフトウェアに加えて、カスタムビルドのソフトウェアにも悪意のあるコードが含まれている可能性があります。これには、ロジックボム、バックドア、および組織のミッション/ビジネス機能に影響を与える可能性のあるその他のタイプのサイバー攻撃などが含まれます。従来の悪意のあるコードに対する保護メカニズムでは、このよ		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	うなコードを常に検出できるとは限りません。このような状況では、組織は代わりに、ソフトウェアが意図した機能以外を実行しないようにするために、安全なコーディング手法、構成の管理と制御、信頼できる調達プロセス、監視方法などの他の保護手段を使用しています。組織は、悪意のあるコードの検出に対応するため、さまざまなアクションが必要であると判断する場合があります。例えば、組織は、定期的なスキャン中の悪意のあるコードの検出に対応するアクション、悪意のあるダウンロードの検出に対応するアクション、および/またはファイルを開いたり実行しようとしたときの悪意のある検出に対応するアクションを定義できます。関連コントロール: CM-3、MP-2、SA-4、SA-		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	8、SA-12、SA-13、SC-7、SC-26、SC-44、SI-2、SI-4、SI-7。参考文献: NIST 特別刊行物 800-83。		
SI-4 (1)	組織は、個々の侵入検知ツールを情報システム全体の侵入検知システムに接続し、設定します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (4)	情報システムは、受信および送信の通信トラフィックを継続的にモニタリングし、異常な、または不正なアクティビティや状態がないことを確認します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (4)	情報システムは、受信および送信の通信トラフィックを継続的にモニタリングし、異常な、または不正なアクティビティや状態がないことを確認します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (4)	情報システムは、受信および送信の通信トラフィックを継続的にモニタリングし、異常な、または不正なアクティビティや状態がないことを確認します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (4)	情報システムは、受信および送信の通信トラフィックを継続的にモニタリングし、異常な、または不正なアクティビティや状態がないことを確認します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	[api-gw-associated-with-waf](#)	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	組織: a。情報システムのセキュリティ警告、勧告、指令を [Assignment: organization-defined external organizations] (割り当て:組織で定義された外部組織) から継続的に受信します。b。必要と判断される内部セキュリティ警告、勧告、指令を作成します。c。セキュリティ警告、勧告、指令を (1 つまたは複数) [Selection(one or more): [Assignment: organization-defined personnel or roles] (選択 (1 つ以上): 割り当て: 組織で定義された担当者またはロール)、[Assignment: organization-defined elements within the organization] (割り当て: 組織で定義した組織内のエレメント)、[Assignment: organization-defined external organizations] (割り当て: 組織で定義された外	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	部組織) に周知します。d。定められた時間枠に従ってセキュリティ指令を実施するか、違反の程度を発行機関に通知します。補足ガイダンス: 米国コンピュータ緊急対応チーム (US-CERT) は、連邦政府全体の状況認識を維持するために、セキュリティ警告と勧告を生成します。セキュリティ指令は、その指令を発行する責任と権限を持つ OMB またはその他の指定機関によって発行されます。これらの指令の多くには重大な性質があり、指令が適時に実施されなければ、組織の運営や資産、個人、その他の組織、および国家に直ちに悪影響を及ぼす可能性があるため、セキュリティ指令の遵守は不可欠です。外部組織には、例えば、外部のミッション/ビジネスパートナー、サプライチェーンパート		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ナー、外部サービスプロバイダー、その他のピア/サポート組織が含まれます。関連コントロール: SI-2 参考文献: NIST 特別刊行物 800-40。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	組織: a。情報システムのセキュリティ警告、勧告、指令を [Assignment: organization-defined external organizations] (割り当て:組織で定義された外部組織) から継続的に受信します。b。必要と判断される内部セキュリティ警告、勧告、指令を作成します。c。セキュリティ警告、勧告、指令を (1 つまたは複数) [Selection(one or more): [Assignment: organization-defined personnel or roles] (選択 (1 つ以上): 割り当て: 組織で定義された担当者またはロール)、[Assignment: organization-defined elements within the organization] (割り当て: 組織で定義した組織内のエレメント)、[Assignment: organization-defined external organizations] (割り当て: 組織で定義された外	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	部組織) に周知します。d。定められた時間枠に従ってセキュリティ指令を実施するか、違反の程度を発行機関に通知します。補足ガイダンス: 米国コンピュータ緊急対応チーム (US-CERT) は、連邦政府全体の状況認識を維持するために、セキュリティ警告と勧告を生成します。セキュリティ指令は、その指令を発行する責任と権限を持つ OMB またはその他の指定機関によって発行されます。これらの指令の多くには重大な性質があり、指令が適時に実施されなければ、組織の運営や資産、個人、その他の組織、および国家に直ちに悪影響を及ぼす可能性があるため、セキュリティ指令の遵守は不可欠です。外部組織には、例えば、外部のミッション/ビジネスパートナー、サプライチェーンパート		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ナー、外部サービスプロバイダー、その他のピア/サポート組織が含まれます。関連コントロール: SI-2 参考文献: NIST 特別刊行物 800-40。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	組織: a。情報システムのセキュリティ警告、勧告、指令を [Assignment: organization-defined external organizations] (割り当て:組織で定義された外部組織) から継続的に受信します。b。必要と判断される内部セキュリティ警告、勧告、指令を作成します。c。セキュリティ警告、勧告、指令を (1 つまたは複数) [Selection(one or more): [Assignment: organization-defined personnel or roles] (選択 (1 つ以上): 割り当て: 組織で定義された担当者またはロール)、[Assignment: organization-defined elements within the organization] (割り当て: 組織で定義した組織内のエレメント)、[Assignment: organization-defined external organizations] (割り当て: 組織で定義された外	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	部組織) に周知します。d。定められた時間枠に従ってセキュリティ指令を実施するか、違反の程度を発行機関に通知します。補足ガイダンス: 米国コンピュータ緊急対応チーム (US-CERT) は、連邦政府全体の状況認識を維持するために、セキュリティ警告と勧告を生成します。セキュリティ指令は、その指令を発行する責任と権限を持つ OMB またはその他の指定機関によって発行されます。これらの指令の多くには重大な性質があり、指令が適時に実施されなければ、組織の運営や資産、個人、その他の組織、および国家に直ちに悪影響を及ぼす可能性があるため、セキュリティ指令の遵守は不可欠です。外部組織には、例えば、外部のミッション/ビジネスパートナー、サプライチェーンパート		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ナー、外部サービスプロバイダー、その他のピア/サポート組織が含まれます。関連コントロール: SI-2 参考文献: NIST 特別刊行物 800-40。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	組織: a。情報システムのセキュリティ警告、勧告、指令を [Assignment: organization-defined external organizations] (割り当て:組織で定義された外部組織) から継続的に受信します。b。必要と判断される内部セキュリティ警告、勧告、指令を作成します。c。セキュリティ警告、勧告、指令を (1 つまたは複数) [Selection(one or more): [Assignment: organization-defined personnel or roles] (選択 (1 つ以上): 割り当て: 組織で定義された担当者またはロール)、[Assignment: organization-defined elements within the organization] (割り当て: 組織で定義した組織内のエレメント)、[Assignment: organization-defined external organizations] (割り当て: 組織で定義された外	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	部組織) に周知します。d。定められた時間枠に従ってセキュリティ指令を実施するか、違反の程度を発行機関に通知します。補足ガイダンス: 米国コンピュータ緊急対応チーム (US-CERT) は、連邦政府全体の状況認識を維持するために、セキュリティ警告と勧告を生成します。セキュリティ指令は、その指令を発行する責任と権限を持つ OMB またはその他の指定機関によって発行されます。これらの指令の多くには重大な性質があり、指令が適時に実施されなければ、組織の運営や資産、個人、その他の組織、および国家に直ちに悪影響を及ぼす可能性があるため、セキュリティ指令の遵守は不可欠です。外部組織には、例えば、外部のミッション/ビジネスパートナー、サプライチェーンパート		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ナー、外部サービスプロバイダー、その他のピア/サポート組織が含まれます。関連コントロール: SI-2 参考文献: NIST 特別刊行物 800-40。		
SI-7 (1)	情報システムは、少なくとも月に 1 回、セキュリティ関連の整合性をチェックするイベントを実行します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7 (1)	情報システムは、少なくとも月に 1 回、セキュリティ関連の整合性をチェックするイベントを実行します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7 (1)	情報システムは、少なくとも月に 1 回、セキュリティ関連の整合性をチェックするイベントを実行します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7	組織は、[Assignment: organization-defined software, firmware, and information (割り当て: 組織で定義されたソフトウェア、ファームウェア、情報)] に対する不正な変更を検出するための整合性検証ツールを採用します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-16	情報システムは、不正なコードの実行からメモリを保護するために [Assignment: organization-defined security safeguards] (割り当て:組織が定めるセキュリティ対策) を実装しています。補足ガイダンス:一部の攻撃者は、実行不可能なメモリ領域または禁止されているメモリ位置でコードを実行することを目的として攻撃を仕掛けます。メモリを保護するために採用されているセキュリティ保護手段には、データ実行防止やアドレス空間配置のランダム化などがあります。データ実行防止の保護手段は、ハードウェアで強制することも、メカニズムの強度を高めるハードウェアを使用してソフトウェアで強制することもできます。関連コントロール:AC-25、SC-3。	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service (Amazon ECS) コンテナで使用できる最大メモリを制限することで、コンテナへの悪意のあるアクセスが発生しても、リソースの使用量が悪用されることはありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	制御: なし。参考: なし。		

テンプレート

テンプレートは、GitHub の「Operational Best Practices for FedRAMP(Moderate)」で入手できます。

FedRAMP (High Part 1) の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Federal Risk and Authorization Management Program (FedRAMP) と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の FedRAMP コントロールに関連付けられます。「FedRAMP」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	elb-acm-certificate-required	POPULATE THIS
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	access-keys-rotated	組織のポリシーに従って IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (12)(a)	組織: a。[Assignment: organization-defined atypical use (割り当て: 組織で定義された非定型の使用)] の情報システムアカウントをモニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (12)(a)	組織: a。[Assignment: organization-defined atypical use (割り当て: 組織で定義された非定型の使用)] の情報システムアカウントをモニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (3)	情報システムは、ユーザーアカウントの非アクティブな状態が 90 日を経過すると、自動的にアカウントを無効にします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (3)	情報システムは、ユーザーアカウントの非アクティブな状態が 90 日を経過すると、自動的にアカウントを無効にします。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員または役割)] に通知します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	access-keys-rotated	組織のポリシーに従って IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	access-keys-rotated	組織のポリシーに従って IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人の IAM ユーザーがあることを確認することで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいて IAM ユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループが少なくとも 1 人の IAM ユーザーを持つようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいて IAM ユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループが少なくとも 1 人の IAM ユーザーを持つようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいて IAM ユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人の IAM ユーザーがあることを確認することで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいて IAM ユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-6(2)	情報システムでは、特権アカウントまたはロール内から操作する際、セキュリティ以外関数へのアクセスにより公開が制限される場合、非特権アカウントの使用が必須となります。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(2)	情報システムでは、特権アカウントまたはロール内から操作する際、セキュリティ以外関数へのアクセスにより公開が制限される場合、非特権アカウントの使用が必須となります。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(2)	情報システムでは、特権アカウントまたはロール内から操作する際、セキュリティ以外関数へのアクセスにより公開が制限される場合、非特権アカウントの使用が必須となります。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。
AC-6(9)	情報システムは、特権関数の実行をログに記録します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	情報システムは、特権関数の実行をログに記録します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	情報システムは、特権関数の実行をログに記録します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	情報システムは、特権関数の実行をログに記録します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
AC-6(9)	情報システムは、特権関数の実行をログに記録します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	情報システムは、特権関数の実行をログに記録します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	情報システムは、特権関数の実行をログに記録します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	情報システムは、特権関数の実行をログに記録します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 (10)	情報システムは、非特権ユーザーが特権的機能を実行して、実装されたセキュリティの保護/対策を無効化、回避、変更することを防ぎます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 (10)	情報システムは、非特権ユーザーが特権的機能を実行して、実装されたセキュリティの保護/対策を無効化、回避、変更することを防ぎます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC-6 (10)	情報システムは、非特権ユーザーが特権的機能を実行して、実装されたセキュリティの保護/対策を無効化、回避、変更することを防ぎます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-11	組織は、セキュリティインシデントの事後調査を支援するため、また、規制および組織の情報保持要件を満たすために、監査レコードを少なくとも 90 日間保持します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	[api-gw-execution-logging-enabled](#)	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-7	情報システムは、監査レコードの削減とレポート生成機能を提供および実装します。これには次のような機能があります。a. オンデマンドの監査レコードのレビュー、分析、報告要件、インシデントの事後調査をサポートします。b. 監査レコードの元のコンテンツや時刻順序は変更されません。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-7	情報システムは、監査レコードの削減とレポート生成機能を提供および実装します。これには次のような機能があります。a. オンデマンドの監査レコードのレビュー、分析、報告要件、インシデントの事後調査をサポートします。b. 監査レコードの元のコンテンツや時刻順序は変更されません。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-7 (1)	情報システムは、[Assignment: organization-defined audit fields within audit records (割り当て: 組織で定義された監査レコード内の監査フィールド)] に基づいて、対象のイベントの監査レコードを処理する機能を提供します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-7 (1)	情報システムは、[Assignment: organization-defined audit fields within audit records (割り当て: 組織で定義された監査レコード内の監査フィールド)] に基づいて、対象のイベントの監査レコードを処理する機能を提供します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。
AU-9	情報システムは、監査情報と監査ツールを不正アクセス、変更、削除から保護します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
AU-9	情報システムは、監査情報と監査ツールを不正アクセス、変更、削除から保護します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9	情報システムは、監査情報と監査ツールを不正アクセス、変更、削除から保護します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9 (2)	情報システムは、少なくとも週に一度、監査記録を監査対象のシステムやコンポーネントとは物理的に異なるシステムまたはシステムコンポーネントにバックアップします。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9 (2)	情報システムは、少なくとも週に一度、監査記録を監査対象のシステムやコンポーネントとは物理的に異なるシステムまたはシステムコンポーネントにバックアップします。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	[api-gw-execution-logging-enabled](#)	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	この情報システムは、[組織が定義したシステムコンポーネントをここに代入] で、AU-2a に定義されているように、システムが監査できるイベントタイプの監査記録生成機能を用意します。b。[組織が定義した担当者またはロールをここに代入] が、システムの特定のコンポーネントによってログに記録されたイベントタイプを選択できるようにします。c。AU-2c で定義されたイベントタイプについて、AU-3 で定義された監査記録の内容を含む監査記録を生成します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-7 (a)	組織: a。重要な機能のみを提供するように情報システムを設定します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-7 (a)	組織: a。重要な機能のみを提供するように情報システムを設定します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
CM-7 (a)	組織: a。重要な機能のみを提供するように情報システムを設定します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (1)	組織は、コンポーネントのインストール、削除、および情報システムの更新において不可欠な部分である情報システムコンポーネントのインベントリを更新します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (1)	組織は、コンポーネントのインストール、削除、および情報システムの更新において不可欠な部分である情報システムコンポーネントのインベントリを更新します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (3)(a)	組織: a。情報システム内に存在する未承認のハードウェア、ソフトウェア、ファームウェアのコンポーネントを検出するため、検出に最大 5 分の遅延をともなう自動化されたメカニズムを継続的に使用します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (3)(a)	組織: a。情報システム内に存在する未承認のハードウェア、ソフトウェア、ファームウェアのコンポーネントを検出するため、検出に最大 5 分の遅延をともなう自動化されたメカニズムを継続的に使用します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (3)(a)	組織: a。情報システム内に存在する未承認のハードウェア、ソフトウェア、ファームウェアのコンポーネントを検出するため、検出に最大 5 分の遅延をともなう自動化されたメカニズムを継続的に使用します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CM-8 (3)(a)	組織: a。情報システム内に存在する未承認のハードウェア、ソフトウェア、ファームウェアのコンポーネントを検出するため、検出に最大 5 分の遅延をともなう自動化されたメカニズムを継続的に使用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6 (1)	組織は、同じ脅威の影響を受けにくくするために、一次保管場所と十分に離れた代替保管場所を特定します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6 (1)	組織は、同じ脅威の影響を受けにくくするために、一次保管場所と十分に離れた代替保管場所を特定します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6 (1)	組織は、同じ脅威の影響を受けにくくするために、一次保管場所と十分に離れた代替保管場所を特定します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6 (1)	組織は、同じ脅威の影響を受けにくくするために、一次保管場所と十分に離れた代替保管場所を特定します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6 (1)	組織は、同じ脅威の影響を受けにくくするために、一次保管場所と十分に離れた代替保管場所を特定します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6 (1)	組織は、同じ脅威の影響を受けにくくするために、一次保管場所と十分に離れた代替保管場所を特定します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-6 (1)	組織は、同じ脅威の影響を受けにくくするために、一次保管場所と十分に離れた代替保管場所を特定します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6 (1)	組織は、同じ脅威の影響を受けにくくするために、一次保管場所と十分に離れた代替保管場所を特定します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	redshift-cluster-maintenancesettings-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	情報システム: a. [組織が定義したシステムコンポーネントをここに代入] に含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。b. システムに含まれるユーザーレベルの情報のバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。c. セキュリティおよびプライバシー関連ドキュメントを含むシステムドキュメントのバックアップを [組織が定義したリカバリ時間とリカバリポイントの目標と整合性のある頻度をここに代入] の頻度で実行します。d. バックアップ情報の機密性、完全性、可用性を保護します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9 (b)	組織: b。情報システムに含まれるシステムレベルの情報のバックアップを実行します (毎日の増分、毎週のすべて)。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2	情報システムは、組織のユーザー (または組織のユーザーに代わって実行するプロセス) を一意に識別し認証します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA-2	情報システムは、組織のユーザー (または組織のユーザーに代わって実行するプロセス) を一意に識別し認証します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)(2)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(2) 情報システムは、非特権アカウントへのネットワークアクセスのための多要素認証を実装します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)(2)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(2) 情報システムは、非特権アカウントへのネットワークアクセスのための多要素認証を実装します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5 (1)(a)(d)(e)	パスワードベースの認証のための情報システム: a。[Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type (割り当て: 組織で定義された大文字と小文字の区別、文字数、大文字、小文字、数字、特殊文字の組み合わせに関する、各タイプの最小要件を含む要件)] のパスワードの複雑さを最小限に抑えます: d。[Assignment: organization- defined numbers for lifetime minimum, lifetime maximum (割り当て: 組織で定義されたライフタイムの最小および最大の数値)] のパスワードの最小および最大有効期間の制限を適用します:	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	e。24 世代にわたるパスワードの再利用の禁止		のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5 (4)	組織は、自動化されたツールを使用して、パスワード認証システムに [Assignment: organization-defined requirements (割り当て: 組織で定義された要件)] を満たす十分な強度があるかどうかを判断します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA-5 (7)	組織は、暗号化されていない静的オーセンティケーターが、アプリケーションやアクセススクリプトに埋め込まれたり、ファンクションキーに割り当てられたりしていないことを確認します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-6 (1)	組織は、セキュリティインシデントの報告をサポートするための自動化されたメカニズムを採用します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-6 (1)	組織は、セキュリティインシデントの報告をサポートするための自動化されたメカニズムを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-6 (1)	組織は、セキュリティインシデントの報告をサポートするための自動化されたメカニズムを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-7 (1)	組織は、インシデント対応に関連する情報およびサポートの可用性を高めるための自動化されたメカニズムを採用します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-7 (1)	組織は、インシデント対応に関連する情報およびサポートの可用性を高めるための自動化されたメカニズムを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-7 (1)	組織は、インシデント対応に関連する情報およびサポートの可用性を高めるための自動化されたメカニズムを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5	組織: a。情報システムおよびホストされているアプリケーションの脆弱性をスキャンし [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process (割り当て: 組織で定義された頻度および/またはプロセスに従ったランダムな頻度)]、システム/アプリケーションに影響を与える可能性のある新たな脆弱性が特定され、報告された場合にもスキャンします: b。ツール間の相互運用性を促進し、脆弱性管理プロセスの一部を自動化するために、以下の標準を使用した脆弱性スキャンツールおよびテクノロジーを採用します: 1。プラットフォーム、ソフトウェアの欠陥、不適切な構成を列挙します: 2。チェックリストとテスト手順	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	のフォーマット: および 3。脆弱性による影響の測定: c。脆弱性スキャンレポートとセキュリティコントロール評価の結果を分析します: d。リスクの組織的評価に従って、正当な脆弱性を修正します: [Assignment: organization-defined response times (割り当て: 組織で定義された応答時間)]: および e。脆弱性スキャンプロセスおよびセキュリティコントロール評価から取得した情報を [Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] と共有し、他の情報システムにおける同様の脆弱性 (システム的な弱点や欠陥) を排除します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5	組織: a。情報システムおよびホストされているアプリケーションの脆弱性を毎月スキャンし [operating system/infrastructure; monthly web applications and databases (オペレーティングシステム/インフラストラクチャ、毎月のウェブアプリケーションおよびデータベース)]、システム/アプリケーションに影響を与える可能性のある新たな脆弱性が特定され、報告された場合にもスキャンします: b。ツール間の相互運用性を促進し、脆弱性管理プロセスの一部を自動化するために、以下の標準を使用した脆弱性スキャンツールおよびテクノロジーを採用します: 1。プラットフォーム、ソフトウェアの欠陥、不適切な構成を列挙します: 2。チェックリストとテスト手順	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	のフォーマット: および 3。脆弱性による影響の測定: c。脆弱性スキャンレポートとセキュリティコントロール評価の結果を分析します: d。正当性のある脆弱性の修正: 組織のリスク評価に基づき、発見日から (30) 日以内に緩和された高リスクの脆弱性、発見日から (90) 日以内に緩和された中程度のリスクの脆弱性、発見日から (180) 日以内に緩和された低リスクの脆弱性: および e。脆弱性スキャンプロセスおよびセキュリティコントロール評価から取得した情報を [Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] と共有し、他の情報システムにおける同様の脆弱性 (システム的な弱点や欠陥) を排除します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、サービスの開発および実装と運用の際に設定管理を行う: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響をドキュメント化する: および e。システム、コンポーネン	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ト、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、サービスの開発および実装と運用の際に設定管理を行う: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響をドキュメント化する: および e。システム、コンポーネン	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ト、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、サービスの開発および実装と運用の際に設定管理を行う: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響をドキュメント化する: および e。システム、コンポーネン	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ト、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、サービスの開発および実装と運用の際に設定管理を行う: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響をドキュメント化する: および e。システム、コンポーネン	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ト、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		
SA-3 (a)	組織: a。情報セキュリティの考慮事項が組み込まれた [Assignment: organization-defined system development life cycle (割り当て: 組織で定義されたシステム開発のライフサイクル)] を使用して、情報システムを管理します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3 (a)	組織: a。情報セキュリティの考慮事項が組み込まれた [Assignment: organization-defined system development life cycle (割り当て: 組織で定義されたシステム開発のライフサイクル)] を使用して、情報システムを管理します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3 (a)	組織: a。情報セキュリティの考慮事項が組み込まれた [Assignment: organization-defined system development life cycle (割り当て: 組織で定義されたシステム開発のライフサイクル)] を使用して、情報システムを管理します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークン、ユーザー名、パスワードが含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはユーザー名とパスワードではなく、OAuth を使用します。
SC-12	組織は、[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] に従って、情報システム内で使用される必要な暗号化の暗号化キーを確立および管理します。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12	組織は、[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] に従って、情報システム内で使用される必要な暗号化の暗号化キーを確立および管理します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12	組織は、[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] に従って、情報システム内で使用される必要な暗号化の暗号化キーを確立および管理します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループが少なくとも 1 人の IAM ユーザーを持つようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいて IAM ユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	情報システムは、通信セッションの信頼性を保護します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23	情報システムは、通信セッションの信頼性を保護します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23	情報システムは、通信セッションの信頼性を保護します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	情報システムは、通信セッションの信頼性を保護します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23	情報システムは、通信セッションの信頼性を保護します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	情報システムは、通信セッションの信頼性を保護します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の機密性と整合性を保護します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4	情報システムは、共有システムリソースを介した不正で意図しない情報転送を防止します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の機密性と完全性を保護します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2 (2)	組織は、欠陥の修復に関する情報システムのコンポーネントの状態を判断するため、少なくとも月に一度、自動化されたメカニズムを採用します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2 (2)	組織は、欠陥の修復に関する情報システムのコンポーネントの状態を判断するため、少なくとも月に一度、自動化されたメカニズムを採用します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2 (2)	組織は、欠陥の修復に関する情報システムのコンポーネントの状態を判断するため、少なくとも月に一度、自動化されたメカニズムを採用します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2 (2)	組織は、欠陥の修復に関する情報システムのコンポーネントの状態を判断するため、少なくとも月に一度、自動化されたメカニズムを採用します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (1)	組織は、個々の侵入検知ツールを情報システム全体の侵入検知システムに接続し、設定します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (4)	情報システムは、受信および送信の通信トラフィックを継続的にモニタリングし、異常な、または不正なアクティビティや状態がないことを確認します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (4)	情報システムは、受信および送信の通信トラフィックを継続的にモニタリングし、異常な、または不正なアクティビティや状態がないことを確認します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (4)	情報システムは、受信および送信の通信トラフィックを継続的にモニタリングし、異常な、または不正なアクティビティや状態がないことを確認します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (4)	情報システムは、受信および送信の通信トラフィックを継続的にモニタリングし、異常な、または不正なアクティビティや状態がないことを確認します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	[api-gw-associated-with-waf](#)	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7	組織は、[Assignment: organization-defined software, firmware, and information (割り当て: 組織で定義されたソフトウェア、ファームウェア、情報)] に対する不正な変更を検出するための整合性検証ツールを採用します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7 (1)	情報システムは、少なくとも月に 1 回、セキュリティ関連の整合性をチェックするイベントを実行します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7 (1)	情報システムは、少なくとも月に 1 回、セキュリティ関連の整合性をチェックするイベントを実行します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7 (1)	情報システムは、少なくとも月に 1 回、セキュリティ関連の整合性をチェックするイベントを実行します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5(1)	組織は、スキャン対象の情報システムの脆弱性を簡単に更新できる機能を含む脆弱性スキャンツールを採用しています。補足ガイダンス: 新しい脆弱性が発見され、発表され、スキャン方法が開発されたときは、スキャン対象の脆弱性をすぐに更新する必要があります。この更新プロセスにより、情報システムの潜在的な脆弱性が可能な限り迅速に特定され、対処されます。関連コントロール: SI-3、SI-7。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5(1)	組織は、スキャン対象の情報システムの脆弱性を簡単に更新できる機能を含む脆弱性スキャンツールを採用しています。補足ガイダンス: 新しい脆弱性が発見され、発表され、スキャン方法が開発されたときは、スキャン対象の脆弱性をすぐに更新する必要があります。この更新プロセスにより、情報システムの潜在的な脆弱性が可能な限り迅速に特定され、対処されます。関連コントロール: SI-3、SI-7。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-5(1)	組織は、スキャン対象の情報システムの脆弱性を簡単に更新できる機能を含む脆弱性スキャンツールを採用しています。補足ガイダンス: 新しい脆弱性が発見され、発表され、スキャン方法が開発されたときは、スキャン対象の脆弱性をすぐに更新する必要があります。この更新プロセスにより、情報システムの潜在的な脆弱性が可能な限り迅速に特定され、対処されます。関連コントロール: SI-3、SI-7。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	組織: (a) 外部通信サービスごとにマネージドインターフェイスを実装し、(b) 各マネージドインターフェイスのトラフィックフローポリシーを確立し、(c) 各インターフェイスで送信される情報の機密性と完全性を保護し、(d) トラフィックフローポリシーに対する各例外を、それを支持するミッション/ビジネスニーズおよびそのニーズの期間を含めて文書化し、(e) トラフィックフローポリシー [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] の例外を確認し、明示的なミッション/ビジネスニーズによって支持されなくなった例外を削除します。補足ガイダンス: 関連コントロール: SC-8。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(5)	マネージドインターフェイスの情報システムは、デフォルトでネットワーク通信トラフィックを拒否し、例外的にネットワーク通信トラフィックを許可します (つまりすべてを拒否し、例外的に許可)。補足ガイダンス: この制御の強化は、インバウンドネットワーク通信トラフィックとアウトバウンドネットワーク通信トラフィックの両方に適用されます。deny-all (すべて拒否)、permit-by-exception (例外による許可) のネットワーク通信トラフィックポリシーでは、必須かつ承認された接続のみが許可されます。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーアカウントを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーアカウントを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーアカウントを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーアカウントを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループが少なくとも 1 人の IAM ユーザーを持つようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいて IAM ユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーアカウントを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(7)	組織: (a) 許可された情報システムへのアクセスと特権をロール別に整理するロールベースのアクセススキームに従って、特権ユーザーアカウントを確立および管理し、(b) 特権的ロールの割り当てを監視し、(c) 特権ロールの割り当てが適切でない場合、[Assignment: organization-defined actions (割り当て: 組織で定義されたアクション)] を実行します。補足ガイダンス: 特権ロールとは、一般ユーザーには実行が許可されていない特定のセキュリティ関連の機能を個人が実行できるようにする、組織が定義したロールで、個人に割り当てられます。これらの特権ロールには、キー管理、アカウント管理、ネットワークおよびシステム管理、データベース管理、ウェブ管理などが含まれます。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-11	情報システム: a。攻撃者が悪用する可能性のある情報を公開することなく、是正措置に必要な情報を提供するエラーメッセージを生成します。b。[Assignment: organization-defined roles](割り当て: 組織で定義された担当者またはロール) にのみエラーメッセージを表示します。補足ガイダンス: 組織はエラーメッセージの構造/内容を慎重に検討します。情報システムがエラー状態をどの程度特定して処理できるかは、組織の方針と運用上の要件によって決まります。攻撃者が悪用する可能性のある情報には、例えば、誤ってユーザー名としてパスワードを入力してログオンを試みた場合、記録された情報から導き出される可能性のあるミッション/ビジネス情報 (明示的に記載	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	されていない場合)、アカウント番号、ソーシャルセキュリティ番号、およびクレジットカード番号などの個人情報が含まれます。さらに、エラーメッセージは情報を送信するための秘密のチャネルを提供する可能性があります。関連コントロール:AU-2、AU-3、SC-31。制御: なし。参考: なし。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3	組織: a。情報システムの入口と出口に悪意のあるコードに対する保護メカニズムを採用して、悪意のあるコードを検出して根絶します。b。組織の構成管理ポリシーと手順に従って、新しいリリースが公開されるたびに、悪意のあるコードに対する保護メカニズムを更新します。c。悪意あるコードの保護機構を 1 に設定します。組織のセキュリティポリシーに従ってファイルがダウンロード、開く、または実行されるときに、情報システム [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] を定期的にスキャンし、[Selection(one or more); endpoint; network entry/exit points (選択 (1 つ以上)、エンドポイント、ネットワークの入口/出	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ロポイント)] で外部ソースからのファイルのリアルタイムスキャンを実行します。2. 悪意のあるコードが検出されると、[Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action] (選択 (1 つ以上): 悪意のあるコードのブロック、悪意のあるコードの隔離、管理者にアラートを送信)、割り当て:組織であるコードのブロが行われます。悪意のあるコードの検出および根絶中に受信する誤検出、およびその結果生じる情報システムの可用性への潜在的な影響に対処します。補足ガイダンス: 情報システムの入口と出口には、ファイアウォール、電子メールサーバー、ウェブサーバー、プロキシサーバー、リモートアク		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	セスサーバー、ワークステーション、ノートパソコン、モバイルデバイスなどが含まれます。悪意のあるコードには、ウイルス、ワーム、トロイの木馬、スパイウェアなどが含まれます。悪意のあるコードは、さまざまな形式 (UUENCODE、Unicode など) でエンコードされたり、圧縮されたファイルや隠しファイルに格納されたり、またはステガノグラフィを使用してファイルに隠されたりすることもあります。悪意のあるコードは、ウェブアクセス、電子メール、電子メールの添付ファイル、ポータブルストレージデバイスなど、さまざまな方法で転送される可能性があります。悪意のあるコードの挿入は、情報システムの脆弱性を悪用することによって行われます。悪意のあるコードに対す		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	る保護メカニズムには、たとえば、ウイルス対策シグネチャの定義やレピュテーションベースの技術が含まれます。悪意のあるコードの影響を制限または排除するためのさまざまな技術や方法が存在します。広範囲にわたる構成管理と包括的なソフトウェアの整合性の制御は、不正なコードの実行を防止するのに効果的な場合があります。市販のソフトウェアに加えて、カスタムビルドのソフトウェアにも悪意のあるコードが含まれている可能性があります。これには、ロジックボム、バックドア、および組織のミッション/ビジネス機能に影響を与える可能性のあるその他のタイプのサイバー攻撃などが含まれます。従来の悪意のあるコードに対する保護メカニズムでは、このようなコードを常に検		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	出できるとは限りません。このような状況では、組織は代わりに、ソフトウェアが意図した機能以外を実行しないようにするために、安全なコーディング手法、構成の管理と制御、信頼できる調達プロセス、監視方法などの他の保護手段を使用しています。組織は、悪意のあるコードの検出に対応するため、さまざまなアクションが必要であると判断する場合があります。例えば、組織は、定期的なスキャン中の悪意のあるコードの検出に対応するアクション、悪意のあるダウンロードの検出に対応するアクション、および/またはファイルを開いたり実行しようとしたときの悪意のある検出に対応するアクションを定義できます。関連コントロール: CM-3、MP-2、SA-4、SA-8、SA-12、S		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	A-13、SC-7 、SC-26、SC -44、SI-2、SI-4、SI-7 。参考文献: NIST 特 別刊行物 800-83。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3	組織: a。情報システムの入口と出口に悪意のあるコードに対する保護メカニズムを採用して、悪意のあるコードを検出して根絶します。b。組織の構成管理ポリシーと手順に従って、新しいリリースが公開されるたびに、悪意のあるコードに対する保護メカニズムを更新します。c。悪意あるコードの保護機構を 1 に設定します。組織のセキュリティポリシーに従ってファイルがダウンロード、開く、または実行されるときに、情報システム [Assignment: organization-defined frequency (割り当て: 組織が定める頻度)] を定期的にスキャンし、[Selection(one or more); endpoint; network entry/exit points (選択 (1 つ以上)、エンドポイント、ネットワークの入口/出	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に AWS Codebuild プロジェクト環境内の個人用アクセストークン、ユーザー名、パスワードが含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはユーザー名とパスワードではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ロポイント)] で外部ソースからのファイルのリアルタイムスキャンを実行します。2. 悪意のあるコードが検出されると、[Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action] (選択 (1 つ以上): 悪意のあるコードのブロック、悪意のあるコードの隔離、管理者にアラートを送信)、割り当て:組織であるコードのブロが行われます。悪意のあるコードの検出および根絶中に受信する誤検出、およびその結果生じる情報システムの可用性への潜在的な影響に対処します。補足ガイダンス: 情報システムの入口と出口には、ファイアウォール、電子メールサーバー、ウェブサーバー、プロキシサーバー、リモートアク		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	セスサーバー、ワークステーション、ノートパソコン、モバイルデバイスなどが含まれます。悪意のあるコードには、ウイルス、ワーム、トロイの木馬、スパイウェアなどが含まれます。悪意のあるコードは、さまざまな形式 (UUENCODE、Unicode など) でエンコードされたり、圧縮されたファイルや隠しファイルに格納されたり、またはステガノグラフィを使用してファイルに隠されたりすることもあります。悪意のあるコードは、ウェブアクセス、電子メール、電子メールの添付ファイル、ポータブルストレージデバイスなど、さまざまな方法で転送される可能性があります。悪意のあるコードの挿入は、情報システムの脆弱性を悪用することによって行われます。悪意のあるコードに対す		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	る保護メカニズムには、たとえば、ウイルス対策シグネチャの定義やレピュテーションベースの技術が含まれます。悪意のあるコードの影響を制限または排除するためのさまざまな技術や方法が存在します。広範囲にわたる構成管理と包括的なソフトウェアの整合性の制御は、不正なコードの実行を防止するのに効果的な場合があります。市販のソフトウェアに加えて、カスタムビルドのソフトウェアにも悪意のあるコードが含まれている可能性があります。これには、ロジックボム、バックドア、および組織のミッション/ビジネス機能に影響を与える可能性のあるその他のタイプのサイバー攻撃などが含まれます。従来の悪意のあるコードに対する保護メカニズムでは、このようなコードを常に検		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	出できるとは限りません。このような状況では、組織は代わりに、ソフトウェアが意図した機能以外を実行しないようにするために、安全なコーディング手法、構成の管理と制御、信頼できる調達プロセス、監視方法などの他の保護手段を使用しています。組織は、悪意のあるコードの検出に対応するため、さまざまなアクションが必要であると判断する場合があります。例えば、組織は、定期的なスキャン中の悪意のあるコードの検出に対応するアクション、悪意のあるダウンロードの検出に対応するアクション、および/またはファイルを開いたり実行しようとしたときの悪意のある検出に対応するアクションを定義できます。関連コントロール: CM-3、MP-2、SA-4、SA-8、SA-12、S		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	A-13、SC-7 、SC-26、SC -44、SI-2、SI-4、SI-7 。参考文献: NIST 特 別刊行物 800-83。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	組織: a。情報システムのセキュリティ警告、勧告、指令を [Assignment: organization-defined external organizations] (割り当て:組織で定義された外部組織) から継続的に受信します。b。必要と判断される内部セキュリティ警告、勧告、指令を作成します。c。セキュリティ警告、勧告、指令を (1 つまたは複数) [Selection(one or more): [Assignment: organization-defined personnel or roles] (選択 (1 つ以上): 割り当て: 組織で定義された担当者またはロール)、[Assignment: organization-defined elements within the organization] (割り当て: 組織で定義した組織内のエレメント)、[Assignment: organization-defined external organizations] (割り当て: 組織で定義された外	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	部組織) に周知します。d。定められた時間枠に従ってセキュリティ指令を実施するか、違反の程度を発行機関に通知します。補足ガイダンス: 米国コンピュータ緊急対応チーム (US-CERT) は、連邦政府全体の状況認識を維持するために、セキュリティ警告と勧告を生成します。セキュリティ指令は、その指令を発行する責任と権限を持つ OMB またはその他の指定機関によって発行されます。これらの指令の多くには重大な性質があり、指令が適時に実施されなければ、組織の運営や資産、個人、その他の組織、および国家に直ちに悪影響を及ぼす可能性があるため、セキュリティ指令の遵守は不可欠です。外部組織には、例えば、外部のミッション/ビジネスパートナー、サプライチェーンパート		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ナー、外部サービスプロバイダー、その他のピア/サポート組織が含まれます。関連コントロール: SI-2 参考文献: NIST 特別刊行物 800-40。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	組織: a。情報システムのセキュリティ警告、勧告、指令を [Assignment: organization-defined external organizations] (割り当て:組織で定義された外部組織) から継続的に受信します。b。必要と判断される内部セキュリティ警告、勧告、指令を作成します。c。セキュリティ警告、勧告、指令を (1 つまたは複数) [Selection(one or more): [Assignment: organization-defined personnel or roles] (選択 (1 つ以上): 割り当て: 組織で定義された担当者またはロール)、[Assignment: organization-defined elements within the organization] (割り当て: 組織で定義した組織内のエレメント)、[Assignment: organization-defined external organizations] (割り当て: 組織で定義された外	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	部組織) に周知します。d。定められた時間枠に従ってセキュリティ指令を実施するか、違反の程度を発行機関に通知します。補足ガイダンス: 米国コンピュータ緊急対応チーム (US-CERT) は、連邦政府全体の状況認識を維持するために、セキュリティ警告と勧告を生成します。セキュリティ指令は、その指令を発行する責任と権限を持つ OMB またはその他の指定機関によって発行されます。これらの指令の多くには重大な性質があり、指令が適時に実施されなければ、組織の運営や資産、個人、その他の組織、および国家に直ちに悪影響を及ぼす可能性があるため、セキュリティ指令の遵守は不可欠です。外部組織には、例えば、外部のミッション/ビジネスパートナー、サプライチェーンパート		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ナー、外部サービスプロバイダー、その他のピア/サポート組織が含まれます。関連コントロール: SI-2 参考文献: NIST 特別刊行物 800-40。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	組織: a。情報システムのセキュリティ警告、勧告、指令を [Assignment: organization-defined external organizations] (割り当て:組織で定義された外部組織) から継続的に受信します。b。必要と判断される内部セキュリティ警告、勧告、指令を作成します。c。セキュリティ警告、勧告、指令を (1 つまたは複数) [Selection(one or more): [Assignment: organization-defined personnel or roles] (選択 (1 つ以上): 割り当て: 組織で定義された担当者またはロール)、[Assignment: organization-defined elements within the organization] (割り当て: 組織で定義した組織内の工レメント)、[Assignment: organization-defined external organizations] (割り当て: 組織で定義された外	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	部組織) に周知します。d。定められた時間枠に従ってセキュリティ指令を実施するか、違反の程度を発行機関に通知します。補足ガイダンス: 米国コンピュータ緊急対応チーム (US-CERT) は、連邦政府全体の状況認識を維持するために、セキュリティ警告と勧告を生成します。セキュリティ指令は、その指令を発行する責任と権限を持つ OMB またはその他の指定機関によって発行されます。これらの指令の多くには重大な性質があり、指令が適時に実施されなければ、組織の運営や資産、個人、その他の組織、および国家に直ちに悪影響を及ぼす可能性があるため、セキュリティ指令の遵守は不可欠です。外部組織には、例えば、外部のミッション/ビジネスパートナー、サプライチェーンパート		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ナー、外部サービスプロバイダー、その他のピア/サポート組織が含まれます。関連コントロール: SI-2 参考文献：NIST 特別刊行物 800-40。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-5	組織: a。情報システムのセキュリティ警告、勧告、指令を [Assignment: organization-defined external organizations] (割り当て:組織で定義された外部組織) から継続的に受信します。b。必要と判断される内部セキュリティ警告、勧告、指令を作成します。c。セキュリティ警告、勧告、指令を (1 つまたは複数) [Selection(one or more): [Assignment: organization-defined personnel or roles] (選択 (1 つ以上): 割り当て: 組織で定義された担当者またはロール)、[Assignment: organization-defined elements within the organization] (割り当て: 組織で定義した組織内のエレメント)、[Assignment: organization-defined external organizations] (割り当て: 組織で定義された外	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	部組織) に周知します。d。定められた時間枠に従ってセキュリティ指令を実施するか、違反の程度を発行機関に通知します。補足ガイダンス: 米国コンピュータ緊急対応チーム (US-CERT) は、連邦政府全体の状況認識を維持するために、セキュリティ警告と勧告を生成します。セキュリティ指令は、その指令を発行する責任と権限を持つ OMB またはその他の指定機関によって発行されます。これらの指令の多くには重大な性質があり、指令が適時に実施されなければ、組織の運営や資産、個人、その他の組織、および国家に直ちに悪影響を及ぼす可能性があるため、セキュリティ指令の遵守は不可欠です。外部組織には、例えば、外部のミッション/ビジネスパートナー、サプライチェーンパート		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ナー、外部サービスプロバイダー、その他のピア/サポート組織が含まれます。関連コントロール: SI-2 参考文献：NIST 特別刊行物 800-40。		
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
AU-12 (a)(c)	情報システム: a。監査機能がデプロイされた/利用可能なすべての情報システムおよびネットワークコンポーネントに、AU-2 a. で定義された監査可能なイベントのための監査レコードの生成機能を提供します。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査することができるかどうかを判断します。成功および失敗したアカウントのログオンイベント、アカウント管理イベント、オブジェクトへのアクセス、ポリシー変更、特権的機能、プロセス追跡、システムイベント。ウェブアプリケーションの場合: すべての管理者によるアクティビティ、認証のチェック、認可のチェック、データの削除、データへのアクセス、データの変更、アクセス許可の変更。d。情報システム内で以下のイベントを監査することを決定します。[organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event (AU-2 a で定義された監査可能なイ	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントの組織定義のサブ集合で、特定された各イベントが継続的に監査される)]。		
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for FedRAMP (High Part 1)」で入手できます。

FedRAMP (High Part 2) の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Federal Risk and Authorization Management Program (FedRAMP) と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の FedRAMP コントロールに関連付けられます。「FedRAMP」によるコントロール

を、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-02 (11)	情報システムは、組織定義のシステムアカウントの組織定義の環境および/または使用状況を適用します。	guardduty-enabled-centralized	Amazon GuardDuty を使用して、IAM インスタンスロールに関連付けられた短期認証情報の使用をモニタリングします。Amazon GuardDuty は、Unautho rizedAccess チェックを使用して、IAM インスタンスプロファイルで認証情報のエクスポートを確認できます。
AC-02 (12)(a)	組織: a。[Assignment: organization-defined atypical use (割り当て: 組織で定義された非定型の使用)] の情報システムアカウントをモニタリングします。	cloudtrail-security-trail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrai

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			l レコードコンテンツ内に表示されます。
AC-06 (03)	組織は、セキュリティプランのアクセスのためにタスクを完了する必要がある場合にのみ、割り当てられた担当者へのネットワークアクセスを許可します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-06 (03)	組織は、[組織が定義した特権コマンドをここに代入] へのネットワークアクセスを [組織が定義したやむを得ない業務上の必要性] のためだけに許可し、その根拠をシステムのセキュリティ計画に文書化します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-06 (03)	組織は、[組織が定義した特権コマンドをここに代入] へのネットワークアクセスを [組織が定義したやむを得ない業務上の必要性] のためだけに許可し、その根拠をシステムのセキュリティ計画に文書化します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-06 (03)	組織は、[組織が定義した特権コマンドをここに代入] へのネットワークアクセスを [組織が定義したやむを得ない業務上の必要性] のためだけに許可し、その根拠をシステムのセキュリティ計画に文書化します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
AC-06 (03)	組織は、[組織が定義した特権コマンドをここに代入] へのネットワークアクセスを [組織が定義したやむを得ない業務上の必要性] のためだけに許可し、その根拠をシステムのセキュリティ計画に文書化します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-06 (03)	組織は、[組織が定義した特権コマンドをここに代入] へのネットワークアクセスを [組織が定義したやむを得ない業務上の必要性] のためだけに許可し、その根拠をシステムのセキュリティ計画に文書化します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
AC-06 (03)	組織は、[組織が定義した特権コマンドをここに代入] へのネットワークアクセスを [組織が定義したやむを得ない業務上の必要性] のためだけに許可し、その根拠をシステムのセキュリティ計画に文書化します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-06 (03)	組織は、[組織が定義した特権コマンドをここに代入] へのネットワークアクセスを [組織が定義したやむを得ない業務上の必要性] のためだけに許可し、その根拠をシステムのセキュリティ計画に文書化します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
AC-06 (03)	組織は、[組織が定義した特権コマンドをここに代入] へのネットワークアクセスを [組織が定義したやむを得ない業務上の必要性] のためだけに許可し、その根拠をシステムのセキュリティ計画に文書化します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-06 (03)	組織は、[組織が定義した特権コマンドをここに代入] へのネットワークアクセスを [組織が定義したやむを得ない業務上の必要性] のためだけに許可し、その根拠をシステムのセキュリティ計画に文書化します。	eks-endpoint-no-public-access	Kubernetes API サーバーエンドポイントにパブリックにアクセスできないようにして、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターへのアクセスを管理します。Kubernetes API サーバーエンドポイントへのパブリックアクセスを制限することで、EKS クラスターとそのリソースへの不正アクセスのリスクを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-05 (02)	情報システムは、割り当てられた監査ログストレージボリュームがリポジトリの最大監査ログストレージ容量の設定割合に達すると、設定された時間内にキーパーソネルに警告を表示します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (04)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (05)	組織は、監査レコードの分析を脆弱性スキャン情報、パフォーマンスデータ、およびシステムモニタリング情報の分析と統合して、不適切または異常なアクティビティを識別する機能をさらに強化します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (05)	組織は、監査記録の分析で、[選択 (1 つまたは複数): 脆弱性スキャン情報、パフォーマンスデータ、システムモニタリング情報、[他のソースから収集した組織定義のデータ/情報をここに代入]] の分析と統合を行い、不適切または異常な活動を特定する能力をさらに強化します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (07)	組織は、監査レコード情報のレビュー、分析、およびレポートに関連するシステムプロセス、ロール、およびユーザーごとに許可されたアクションを指定します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-06 (07)	組織は、監査レコード情報のレビュー、分析、およびレポートに関連する各 [選択 (1 つまたは複数): システムプロセス、ロール、ユーザー] に対して許可されるアクションを指定します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-09 (02)	情報システムは、監査情報および監査ツールの完全性を保護するための暗号化メカニズムを実装します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
AU-09 (02)	情報システムは、監査情報および監査ツールの完全性を保護するための暗号化メカニズムを実装します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-09 (02)	情報システムは、監査情報および監査ツールの完全性を保護するための暗号化メカニズムを実装します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
AU-09 (02)	情報システムは、監査情報および監査ツールの完全性を保護するための暗号化メカニズムを実装します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-09 (03)	情報システムは、個人が実行したという反論の余地のない証拠を提供します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
AU-09 (03)	情報システムは、監査ログデータへのネットワークアクセスを制限します。	cloudtrail-s3-bucket-public-access-prohibited	CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-10	情報システムは、個人 (または個人を代行するプロセス) が [否認防止の対象として組織が定義するアクションをここに代入] を行ったという反論の余地のない証拠を提供します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
AU-10	情報システムは、個人 (または個人を代行するプロセス) が [否認防止の対象として組織が定義するアクションをここに代入] を行ったという反論の余地のない証拠を提供します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-10	情報システムは、個人 (または個人を代行するプロセス) が [否認防止の対象として組織が定義するアクションをここに代入] を行ったという反論の余地のない証拠を提供します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	組織は、[組織が定義したシステムコンポーネントをここに代入] からの監査記録を、[監査証跡に含まれる個々の記録のタイムスタンプ間の関係について、組織が定義した許容レベルをここに代入] の範囲内で時間相関のあるシステム全体の (論理的または物理的な) 監査証跡にコンパイルします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	組織は、[組織が定義したシステムコンポーネントをここに代入] からの監査記録を、[監査証跡に含まれる個々の記録のタイムスタンプ間の関係について、組織が定義した許容レベルをここに代入] の範囲内で時間相関のあるシステム全体の (論理的または物理的な) 監査証跡にコンパイルします。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。
AU-12	組織は、[組織が定義したシステムコンポーネントをここに代入] からの監査記録を、[監査証跡に含まれる個々の記録のタイムスタンプ間の関係について、組織が定義した許容レベルをここに代入] の範囲内で時間相関のあるシステム全体の (論理的または物理的な) 監査証跡にコンパイルします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	組織は、[組織が定義したシステムコンポーネントをここに代入] からの監査記録を、[監査証跡に含まれる個々の記録のタイムスタンプ間の関係について、組織が定義した許容レベルをここに代入] の範囲内で時間相関のあるシステム全体の (論理的または物理的な) 監査証跡にコンパイルします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	組織は、[組織が定義したシステムコンポーネントをここに代入] からの監査記録を、[監査証跡に含まれる個々の記録のタイムスタンプ間の関係について、組織が定義した許容レベルをここに代入] の範囲内で時間相関のあるシステム全体の (論理的または物理的な) 監査証跡にコンパイルします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	組織は、[組織が定義したシステムコンポーネントをここに代入] からの監査記録を、[監査証跡に含まれる個々の記録のタイムスタンプ間の関係について、組織が定義した許容レベルをここに代入] の範囲内で時間相関のあるシステム全体の (論理的または物理的な) 監査証跡にコンパイルします。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	組織は、[組織が定義したシステムコンポーネントをここに代入] からの監査記録を、[監査証跡に含まれる個々の記録のタイムスタンプ間の関係について、組織が定義した許容レベルをここに代入] の範囲内で時間相関のあるシステム全体の (論理的または物理的な) 監査証跡にコンパイルします。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-12	組織は、[組織が定義したシステムコンポーネントをここに代入] からの監査記録を、[監査証跡に含まれる個々の記録のタイムスタンプ間の関係について、組織が定義した許容レベルをここに代入] の範囲内で時間相関のあるシステム全体の (論理的または物理的な) 監査証跡にコンパイルします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	組織は、[組織が定義したシステムコンポーネントをここに代入] からの監査記録を、[監査証跡に含まれる個々の記録のタイムスタンプ間の関係について、組織が定義した許容レベルをここに代入] の範囲内で時間相関のあるシステム全体の (論理的または物理的な) 監査証跡にコンパイルします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-03	組織は、構成管理されるシステムに対する変更のタイプを決定し、文書化します。b。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-08 (02)	組織は、[組織が定義した自動化メカニズムをここに代入] を使用して、システムの基本構成の最新性、完全性、正確性、可用性を維持します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-08 (02)	組織は、[組織が定義した自動化メカニズムをここに代入] を使用して、システムの基本構成の最新性、完全性、正確性、可用性を維持します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-08 (02)	組織は、[組織が定義した自動化メカニズムをここに代入] を使用して、システムの基本構成の最新性、完全性、正確性、可用性を維持します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-02 (05)	組織は、業務継続性の損失を最小限にとどめ、あるいは全く失わずに、ミッションとビジネス機能を継続するための計画を提供し、一次処理施設やストレージ施設においてシステムが完全に復旧するまで、その継続性を維持します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	リカバリポイントが、指定した期間より前に期限切れになるかどうかを確認します。組織は、緊急時対応計画の一環として復旧時間と復旧ポイントの目的を確立します。代替ストレージサイトの設定には、物理的な施設と、アクセシビリティと正しい実行を保証する復旧オペレーションをサポートするシステムが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	rds-in-backup-plan	Amazon Relational Database Service (Amazon RDS) データベースが AWS Backup プランに存在するかどうかを確認します。組織は、緊急時対応計画の一環として復旧時間と復旧ポイントの目的を確立します。代替ストレージサイトの設定には、物理的な施設と、アクセシビリティと正しい実行を保証する復旧オペレーションをサポートするシステムが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	dynamodb-in-backup-plan	Amazon DynamoDB テーブルが AWS Backup Plans に存在するかどうかを確認します。組織は、緊急時対応計画の一環として復旧時間と復旧ポイントの目的を確立します。代替ストレージサイトの設定には、物理的な施設と、アクセシビリティと正しい実行を保証する復旧オペレーションをサポートするシステムが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-06 (02)	組織は、代替ストレージサイトを設定し、復旧時間と復旧ポイントの目標に沿った復旧作業を促進します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-07 (01)	組織は、同じ脅威の影響を受けにくくするために、一次処理サイトと十分に離れた代替処理サイトを特定します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-07 (04)	組織は、サイトが重要なミッションとビジネス機能をサポートする運用サイトとして機能することができるように、代替処理サイトを準備します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
CP-07 (04)	組織は、サイトが重要なミッションとビジネス機能をサポートする運用サイトとして機能することができるように、代替処理サイトを準備します。	バックアップ/リカバリ・ポイント暗号化	リカバリポイントが暗号化されているかどうかを確認します。サイトの準備では、プライマリサイトのこのような設定の要件と一致する代替処理サイトのシステムの設定の確立したり、重要な供給品と物流上の考慮事項を確実に設定したりします。
CP-07 (04)	組織は、サイトが重要なミッションとビジネス機能をサポートする運用サイトとして機能することができるように、代替処理サイトを準備します。	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されているかどうかを確認します。サイトの準備では、プライマリサイトのこのような設定の要件と一致する代替処理サイトのシステムの設定の確立したり、重要な供給品と物流上の考慮事項を確実に設定したりします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-07 (04)	組織は、サイトが重要なミッションとビジネス機能をサポートする運用サイトとして機能することができるように、代替処理サイトを準備します。	s3-bucket-cross-region-replication-enabled	Amazon S3 バケットに対して S3 クロスリージョンレプリケーションを有効にしたかどうかを確認します。サイトの準備では、プライマリサイトのこのような設定の要件と一致する代替処理サイトのシステムの設定の確立したり、重要な供給品と物流上の考慮事項を確実に設定したりします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	リカバリポイントが、指定した期間より前に期限切れになるかどうかを確認します。重要な情報の個別のストレージは、バックアップストレージメディアのタイプに関係なく、すべての重要な情報に適用されます。重要なシステムソフトウェアには、オペレーティングシステム、ミドルウェア、暗号化キー管理システム、侵入検出システムなどがあります。セキュリティ関連情報には、システムハードウェア、ソフトウェア、ファームウェアコンポーネントのインベントリなどがあります。地理的に分散されたアーキテクチャを含む代替ストレージサイトは、組織の個別の保管施設として機能します。組織は、代替ストレージサイト (データセンターなど) に自動バックアッププロ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			セスを実装することで、個別のストレージを提供することができます。米国共通役務庁 (General Services Administration、GSA) は、セキュリティおよび耐火性コンテナの標準と仕様を確立します。
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	s3-resources-protected-by-backup-plan	データのバックアッププロセスを支援するために、Amazon Simple Storage Service (Amazon S3) バケットが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (03)	組織は、[組織が定義した重要なシステムソフトウェアおよびその他のセキュリティ関連情報をここに代入] のバックアップコピーを別の施設または運用システムとコロケーションされていない耐火性コンテナに保存します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
CP-09 (05)	組織は、システムバックアップ情報を代替ストレージサイト [回復時間および回復時点目標に一致する、組織が定義した期間および転送速度をここに代入] に転送します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (05)	組織は、システムバックアップ情報を代替ストレージサイト [回復時間および回復時点目標に一致する、組織が定義した期間および転送速度をここに代入] に転送します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	リカバリポイントが、指定した期間より前に期限切れになるかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (05)	組織は、システムバックアップ情報を代替ストレージサイト [回復時間および回復時点目標に一致する、組織が定義した期間および転送速度をここに代入] に転送します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
CP-09 (05)	組織は、システムバックアップ情報を代替ストレージサイト [回復時間および回復時点目標に一致する、組織が定義した期間および転送速度をここに代入] に転送します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-09 (05)	組織は、システムバックアップ情報を代替ストレージサイト [回復時間および回復時点目標に一致する、組織が定義した期間および転送速度をここに代入] に転送します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CP-09 (08)	組織は、暗号化メカニズムを使用して、バックアップ情報の不正な開示を防ぎます。	バックアップ/リカバリ・ポイント暗号化	暗号化メカニズムの選択は、バックアップ情報の機密性と完全性を保護する必要性に基づいています。選択したメカニズムの強度は、セキュリティカテゴリまたは情報の分類に見合っています。暗号化保護は、プライマリロケーションと代替ロケーションの両方のストレージ内のシステムバックアップ情報に適用されます。保管中の情報を保護するための暗号化メカニズムを実装する組織も、暗号化キー管理ソリューションを検討します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10 (04)	組織は、[組織が定義した復旧時間をここに代入] 内のシステムコンポーネントを、コンポーネントの既知の運用状態を表す設定制御および完全性保護された情報から復元する機能を提供します。	バックアップ/リカバリ・ポイント暗号化	このルールを有効にして、リカバリポイントが暗号化されているかどうかを確認します。
CP-10 (04)	組織は、[組織が定義した復旧時間をここに代入] 内のシステムコンポーネントを、コンポーネントの既知の運用状態を表す設定制御および完全性保護された情報から復元する機能を提供します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	このルールを有効にして、復旧ポイントの有効期限が指定された期間より後にならない場合に確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10 (04)	組織は、[組織が定義した復旧時間をここに代入] 内のシステムコンポーネントを、コンポーネントの既知の運用状態を表す設定制御および完全性保護された情報から復元する機能を提供します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
CP-10 (04)	組織は、[組織が定義した復旧時間をここに代入] 内のシステムコンポーネントを、コンポーネントの既知の運用状態を表す設定制御および完全性保護された情報から復元する機能を提供します。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10 (04)	組織は、[組織が定義した復旧時間をここに代入] 内のシステムコンポーネントを、コンポーネントの既知の運用状態を表す設定制御および完全性保護された情報から復元する機能を提供します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-02 (02)	非特権アカウントへのアクセスに多要素認証を導入します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-02 (02)	非特権アカウントへのアクセスに多要素認証を導入します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-02 (06)	情報システムは、[選択 (1 つまたは複数): ローカル、ネットワーク、リモート] にアクセスする多要素認証を、[選択 (1 つまたは複数): 特権アカウント、非特権アカウント] へのアクセスに導入します。(a) アクセスを取得するシステムとは別のデバイスによって要素の 1 つを提供する、(b) そのデバイスが [組織が定義したメカニズム強度の要件をここに代入] を満たしていること。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-02 (06)	情報システムは、[選択 (1 つまたは複数): ローカル、ネットワーク、リモート] にアクセスする多要素認証を、[選択 (1 つまたは複数): 特権アカウント、非特権アカウント] へのアクセスに導入します。(a) アクセスを取得するシステムとは別のデバイスによって要素の 1 つを提供する、(b) そのデバイスが [組織が定義したメカニズム強度の要件をここに代入] を満たしていること。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-02 (08)	情報システムは、[選択 (1 つまたは複数): 特権アカウント、非特権アカウント] へのアクセスに、再生不能な認証メカニズムを実装します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-05 (08)	情報システムは、個人が複数のシステムにアカウントを持つことによる漏洩リスクを管理するために、[組織が定義したセキュリティ統制をここに代入] を実装します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA-05 (08)	情報システムは、個人が複数のシステムにアカウントを持つことによる漏洩リスクを管理するために、[組織が定義したセキュリティ統制をここに代入] を実装します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-05 (08)	情報システムは、個人が複数のシステムにアカウントを持つことによる漏洩リスクを管理するために、[組織が定義したセキュリティ統制をここに代入] を実装します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-05 (08)	情報システムは、個人が複数のシステムにアカウントを持つことによる漏洩リスクを管理するために、[組織が定義したセキュリティ統制をここに代入] を実装します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-05 (08)	情報システムは、個人が複数のシステムにアカウントを持つことによる漏洩リスクを管理するために、[組織が定義したセキュリティ統制をここに代入] を実装します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-05 (08)	情報システムは、個人が複数のシステムにアカウントを持つことによる漏洩リスクを管理するために、[組織が定義したセキュリティ統制をここに代入] を実装します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、IAM ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-04 (04)	組織は、インシデントの認識と対応に関する組織全体の視点を達成するために、インシデント情報と個々のインシデント対応を関連付ける自動メカニズムを採用しています。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-04 (04)	組織は、インシデントの認識と対応に関する組織全体の視点を達成するために、インシデント情報と個々のインシデント対応を関連付ける自動メカニズムを採用しています。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
IR-04 (04)	組織は、インシデントの認識と対応に関する組織全体の視点を達成するために、インシデント情報と個々のインシデント対応を関連付ける自動メカニズムを採用しています。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-04 (04)	組織は、インシデントの認識と対応に関する組織全体の視点を達成するために、インシデント情報と個々のインシデント対応を関連付ける自動メカニズムを採用しています。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-04 (04)	組織は、インシデントの認識と対応に関する組織全体の視点を達成するために、インシデント情報と個々のインシデント対応を関連付ける自動メカニズムを採用しています。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。
RA-05	ホストされているアプリケーションをモニタリングおよびスキャンし、脆弱性を検出します。また、システムに影響を及ぼす可能性のある新たな脆弱性が確認された場合は報告します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-05	脆弱性スキャンの範囲の幅と深さを定義します。	inspector-lambda-standard-scan-enabled	ソフトウェアの潜在的な脆弱性を検出するために、Amazon Inspector V2 Lambda 標準スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。Lambda 標準スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。
RA-05	脆弱性スキャンの範囲の幅と深さを定義します。	inspector-ec2-scan-enabled	EC2 インスタンスで潜在的な脆弱性とネットワーク到達可能性の問題を検出するために、Amazon Inspector V2 EC2 スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。EC2 スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-05	脆弱性スキャンの範囲の幅と深さを定義します。	inspector-ecr-scan-enabled	コンテナイメージの潜在的なソフトウェアの脆弱性を検出するために、Amazon Inspector V2 ECR スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。ECR スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。
RA-05 (03)	脆弱性スキャンの範囲の幅と深さを定義します。	inspector-lambda-standard-scan-enabled	ソフトウェアの潜在的な脆弱性を検出するために、Amazon Inspector V2 Lambda 標準スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。Lambda 標準スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-05 (03)	脆弱性スキャンの範囲の幅と深さを定義します。	inspector-ec2-scan-enabled	EC2 インスタンスで潜在的な脆弱性とネットワーク到達可能性の問題を検出するために、Amazon Inspector V2 EC2 スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。EC2 スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。
RA-05 (03)	脆弱性スキャンの範囲の幅と深さを定義します。	inspector-ecr-scan-enabled	コンテナイメージの潜在的なソフトウェアの脆弱性を検出するために、Amazon Inspector V2 ECR スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。ECR スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-05 (05)	[組織が定義したシステムコンポーネントをここに代入] への特権アクセス認証を実装して、組織のスキャンを行います。(認証とすべてのスキャンをサポートするすべてのコンポーネントを指定します)	inspector-ec2-scan-enabled	EC2 インスタンスで潜在的な脆弱性とネットワーク到達可能性の問題を検出するために、Amazon Inspector V2 EC2 スキャンがシングルアカウント環境またはマルチアカウント環境でアクティブ化されているかどうかを確認します。EC2 スキャンが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10	組織は、システム、システムコンポーネント、システムサービスのデベロッパーに以下を要求します: a. システム、コンポーネント、またはサービスを [設計、開発、実装、運用、廃棄の中から 1 つまたは複数を選択] する際に構成管理を実行する。b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティとプライバシーへの影響を文	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	書化する。e。システム、コンポーネント、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-07 (12)	組織は、[組織が定義したホストベースの境界保護メカニズムをここに代入] を [組織が定義したシステムコンポーネントをここに代入] に実装します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-07 (20)	[Assignment: organization-defined system components] を他のシステムコンポーネントから動的に分離する機能を提供します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-07 (21)	境界保護メカニズムを使用して、[Assignment: organization-defined missions and/or business functions] をサポートする [Assignment: organization-defined missions and/or business functions] を分離します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-07(21)	境界保護メカニズムを使用して、[Assignment: organization-defined missions and/or business functions] をサポートする [Assignment: organization-defined missions and/or business functions] を分離します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12 (01)	以下のキーの管理要件 [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction (割り当て: 組織で定義されたキーの生成、配布、保存、アクセス、破棄に関する要件)] に従って、システム内で使用される必要な暗号化の暗号化キーを確立しおよび管理します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28 (01)	組織は、[組織が定義したシステムコンポーネントまたはメディアをここに代入]: [組織が定義した情報をここに代入] で、静止状態にある以下の情報の不正な開示や改変を防ぐための暗号化メカニズムを実装します。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (12)	セキュリティまたはプライバシーに影響を及ぼす不適切または異常な活動に関する以下の兆候が発生した場合、[Assignment: organization-defined automated mechanisms] を使用して、[Assignment: organization-defined personnel or roles] に警告します。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (20)	特権ユーザーに対する以下の追加モニタリングを実施します: [Assignment: organization-defined additional monitoring]。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (20)	特権ユーザーに対する以下の追加モニタリングを実施します: [Assignment: organization-defined additional monitoring]。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (20)	特権ユーザーに対する以下の追加モニタリングを実施します: [Assignment: organization-defined additional monitoring]。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (20)	特権ユーザーに対する以下の追加モニタリングを実施します: [Assignment: organization-defined additional monitoring]。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 AWS アカウント内の API コールアクティビティの詳細が提供されます。
SI-04 (20)	特権ユーザーに対する以下の追加モニタリングを実施します: [Assignment: organization-defined additional monitoring]。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (20)	特権ユーザーに対する以下の追加モニタリングを実施します: [Assignment: organization-defined additional monitoring]。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。
SI-04 (20)	特権ユーザーに対する以下の追加モニタリングを実施します: [Assignment: organization-defined additional monitoring]。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (20)	特権ユーザーに対する以下の追加モニタリングを実施します: [Assignment: organization-defined additional monitoring]。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (20)	特権ユーザーに対する以下の追加モニタリングを実施します: [Assignment: organization-defined additional monitoring]。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (22)	(a) [組織が定義した許可や承認のプロセスをここに代入] で許可または承認されていないネットワークサービスを検出します。(b) 検出された場合、[「監査」、「[組織が定義した担当者またはロールをここに代入] に警告」の 1 つまたは複数を選択] します。	securityhub-enabled	(A) AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (22)	(a) [組織が定義した許可や承認のプロセスをここに代入] で許可または承認されていないネットワークサービスを検出します。(b) 検出された場合、[「監査」、「[組織が定義した担当者またはロールをここに代入] に警告」の 1 つまたは複数を選択] します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-04 (22)	(a) [組織が定義した許可や承認のプロセスをここに代入] で許可または承認されていないネットワークサービスを検出します。(b) 検出された場合、[「監査」、「[組織が定義した担当者またはロールをここに代入] に警告」の 1 つまたは複数を選択] します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-05 (01)	[Assignment: organization-defined automated mechanisms] を使用してセキュリティ警告と注意喚起情報を組織全体に配信します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-05 (01)	[Assignment: organization-defined automated mechanisms] を使用してセキュリティ警告と注意喚起情報を組織全体に配信します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-07 (02)	完全性の検証中に不一致が見つかったときに [組織が定義した担当者または役職をここに代入] に通知する自動ツールを使用します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-07 (02)	完全性の検証中に不一致が見つかったときに [組織が定義した担当者または役職をここに代入] に通知する自動ツールを使用します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-07 (05)	完全性違反が検出されると、自動的に [選択 (1 つまたは複数): システムのシャットダウン、システムの再起動、[組織が定義した統制をここに代入] の実装] を行います。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-07 (05)	完全性違反が検出されると、自動的に [選択 (1 つまたは複数): システムのシャットダウン、システムの再起動、[組織が定義した統制をここに代入] の実装] を行います。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
SI-07 (15)	インストール前に、暗号化メカニズムを実装して、次のソフトウェアまたはファームウェアコンポーネントを認証します: [組織が定義したソフトウェアまたはファームウェアコンポーネントをここに代入]。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-07 (15)	インストール前に、暗号化メカニズムを実装して、次のソフトウェアまたはファームウェアコンポーネントを認証します: [組織が定義したソフトウェアまたはファームウェアコンポーネントをここに代入]。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for FedRAMP (High Part 2)」で入手できます。

FFIEC に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、連邦金融機関審査評議会 (FFIEC) の「Cyber Security Assessment Tool」ドメインと AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソー

スに適用され、1 つ以上の FFIEC サイバーセキュリティ評価ツールコントロールに関連付けられます。FFIEC の「Cyber Security Assessment Tool」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.G.IT.B.1	組織のアセット (例: 外部でホストされているハードウェア、ソフトウェア、データ、システム) のインベントリが維持されます。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
D1.G.IT.B.1	組織のアセット (例: 外部でホストされているハードウェア、ソフトウェア、データ、システム) のイン	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ベントリが維持されます。		数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
D1.G.IT.B.1	組織のアセット (例: 外部でホストされているハードウェア、ソフトウェア、データ、システム) のインベントリが維持されます。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.G.IT.B.1	組織のアセット (例: 外部でホストされているハードウェア、ソフトウェア、データ、システム) のインベントリが維持されます。	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.Rm.B.1	公共施設内には、情報セキュリティおよび事業継続性のリスク管理機能が存在します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.RM.RA.B.2	リスク評価では、追加の認証管理を必要とするインターネットベースのシステムや高リスクの取引が特定されます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
D1.RM.RA.B.2	リスク評価では、追加の認証管理を必要とするインターネットベースのシステムや高リスクの取引が特定されます。	annual-risk-assessment-performed (process check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.TC.Tr.B.2	情報セキュリティに関する年次研修には、インシデント対応、最新のサイバー脅威(例: フィッシング、スピアフィッシング、ソーシャルエンジニアリング、モバイルセキュリティ)、および新たな問題が含まれています。	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
D2.IS.Is.B.1	情報セキュリティの脅威が収集され、適切な社内の従業員と共有されます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.IS.Is.B.1	情報セキュリティの脅威が収集され、適切な社内の従業員と共有されます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.IS.Is.B.1	情報セキュリティの脅威が収集され、適切な社内の従業員と共有されます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
D2.MA.Ma.B.1	監査ログレコードやその他のセキュリティイベントログは、安全な方法で確認され、保持されます。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.MA.Ma.B.2	コンピュータのイベントログは、イベント発生後の調査に使用されます。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.TI.Ti.B.1	公共施設は、脅威に関する情報を提供する、脅威と脆弱性の情報共有元 (例: FS-ISAC、US- CERT) に所属またはサブスクライブします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.TI.Ti.B.1	公共施設は、脅威に関する情報を提供する、脅威と脆弱性の情報共有元 (例: FS-ISAC、US- CERT) に所属またはサブスクライブします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
D2.TI.Ti.B.2	脅威に関する情報は、脅威と脆弱性をモニタリングするために使用されます。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.TI.Ti.B.2	脅威に関する情報は、脅威と脆弱性をモニタリングするために使用されます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.TI.Ti.B.2	脅威に関する情報は、脅威と脆弱性をモニタリングするために使用されます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.TI.Ti.B.3	脅威に関する情報は、内部のリスク管理と統制を強化するために使用されます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D2.TI.Ti.B.3	脅威に関する情報は、内部のリスク管理と統制を強化するために使用されます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
D3.CC.PM.B.1	パッチ管理プログラムが実装され、ソフトウェアおよびファームウェアのパッチが適時に適用されるようにします。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.CC.PM.B.1	パッチ管理プログラムが実装され、ソフトウェアおよびファームウェアのパッチが適時に適用されるようにします。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。
D3.CC.PM.B.1	パッチ管理プログラムが実装され、ソフトウェアおよびファームウェアのパッチが適時に適用されるようにします。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.CC.PM.B.1	パッチ管理プログラムが実装され、ソフトウェアおよびファームウェアのパッチが適時に適用されるようにします。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.CC.PM.B.3	パッチ管理レポートが確認され、欠落しているセキュリティパッチが反映されます。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
D3.CC.PM.B.3	パッチ管理レポートが確認され、欠落しているセキュリティパッチが反映されます。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.CC.PM.B.3	パッチ管理レポートが確認され、欠落しているセキュリティパッチが反映されます。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.CC.PM.B.3	パッチ管理レポートが確認され、欠落しているセキュリティパッチが反映されます。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.1	公共施設では、環境全体をモニタリングすることで異常なアクティビティを検出することができます。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.1	公共施設では、環境全体をモニタリングすることで異常なアクティビティを検出することができます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.1	公共施設では、環境全体をモニタリングすることで異常なアクティビティを検出することができます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.2	異常なアクティビティのアラートを生成する顧客トランザクションがモニタリングされ、レビューされます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.2	異常なアクティビティのアラートを生成する顧客トランザクションがモニタリングされ、レビューされます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.3	物理的アクセスおよび論理的アクセスのログは、以下のイベントでレビューされます。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
D3.DC.An.B.4	サードパーティによる重要なシステムへのアクセスに、不正または異常なアクティビティがないかモニタリングされます。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.An.B.5	昇格された特権がモニタリングされます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
D3.DC.An.B.5	昇格された特権がモニタリングされます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.1	通常のネットワークアクティビティのベースラインが確立されます。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。
D3.DC.Ev.B.1	通常のネットワークアクティビティのベースラインが確立されます。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
D3.DC.Ev.B.1	通常のネットワークアクティビティのベースラインが確立されます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.1	通常のネットワークアクティビティのベースラインが確立されます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.1	通常のネットワークアクティビティのベースラインが確立されます。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
D3.DC.Ev.B.1	通常のネットワークアクティビティのベースラインが確立されます。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.1	通常のネットワークアクティビティのベースラインが確立されます。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.1	通常のネットワークアクティビティのベースラインが確立されます。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.1	通常のネットワークアクティビティのベースラインが確立されます。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.2	潜在的な攻撃を管理者に警告するメカニズム (例: ウイルス対策アラート、ログイベントアラート) が用意されています。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.3	権限のないユーザー、デバイス、接続、およびソフトウェアの存在をモニタリングするプロセスが用意されています。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.3	権限のないユーザー、デバイス、接続、およびソフトウェアの存在をモニタリングするプロセスが用意されています。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.3	権限のないユーザー、デバイス、接続、およびソフトウェアの存在をモニタリングするプロセスが用意されています。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Ev.B.3	権限のないユーザー、デバイス、接続、およびソフトウェアの存在をモニタリングするプロセスが用意されています。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Th.B.1	外部向けシステムと内部ネットワークのリスク評価に従って、独立したテスト (侵入テストと脆弱性スキャンを含む) が実施されます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Th.B.1	外部向けシステムと内部ネットワークのリスク評価に従って、独立したテスト (侵入テストと脆弱性スキャンを含む) が実施されます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.DC.Th.B.1	外部向けシステムと内部ネットワークのリスク評価に従って、独立したテスト (侵入テストと脆弱性スキャンを含む) が実施されます。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.1	従業員は、職務責任と最小権限の原則に基づいて、システムおよび機密データへのアクセス許可が付与されます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.10	本番環境と非本番環境は、情報アセットへの不正アクセスや変更を防止するため、分離されています。(* 公共施設または公共施設のサードパーティに本番環境が存在しない場合は該当しません)	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.10	本番環境と非本番環境は、情報アセットへの不正アクセスや変更を防止するため、分離されています。(* 公共施設または公共施設のサードパーティに本番環境が存在しない場合は該当しません)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.10	本番環境と非本番環境は、情報アセットへの不正アクセスや変更を防止するため、分離されています。(* 公共施設または公共施設のサードパーティに本番環境が存在しない場合は該当しません)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.10	本番環境と非本番環境は、情報アセットへの不正アクセスや変更を防止するため、分離されています。(* 公共施設または公共施設のサードパーティに本番環境が存在しない場合は該当しません)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.12	すべてのパスワードは、保管中および転送中に暗号化されます。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
D3.PC.Am.B.13	機密データは、パブリックネットワークまたは信頼できないネットワーク (例: インターネット) を介して送信される場合に暗号化されます。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.13	機密データは、パブリックネットワークまたは信頼できないネットワーク (例: インターネット) を介して送信される場合に暗号化されます。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
D3.PC.Am.B.13	機密データは、パブリックネットワークまたは信頼できないネットワーク (例: インターネット) を介して送信される場合に暗号化されます。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.13	機密データは、パブリックネットワークまたは信頼できないネットワーク (例: インターネット) を介して送信される場合に暗号化されます。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
D3.PC.Am.B.13	機密データは、パブリックネットワークまたは信頼できないネットワーク (例: インターネット) を介して送信される場合に暗号化されます。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
D3.PC.Am.B.13	機密データは、パブリックネットワークまたは信頼できないネットワーク (例: インターネット) を介して送信される場合に暗号化されます。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.13	機密データは、パブリックネットワークまたは信頼できないネットワーク (例: インターネット) を介して送信される場合に暗号化されます。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
D3.PC.Am.B.15	従業員、請負業者、およびサードパーティによる重要なシステムへのリモートアクセスでは、暗号化された接続と多要素認証を使用します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.15	従業員、請負業者、およびサードパーティによる重要なシステムへのリモートアクセスでは、暗号化された接続と多要素認証を使用します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.15	従業員、請負業者、およびサードパーティによる重要なシステムへのリモートアクセスでは、暗号化された接続と多要素認証を使用します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.15	従業員、請負業者、およびサードパーティによる重要なシステムへのリモートアクセスでは、暗号化された接続と多要素認証を使用します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.15	従業員、請負業者、およびサードパーティによる重要なシステムへのリモートアクセスでは、暗号化された接続と多要素認証を使用します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
D3.PC.Am.B.15	従業員、請負業者、およびサードパーティによる重要なシステムへのリモートアクセスでは、暗号化された接続と多要素認証を使用します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
D3.PC.Am.B.15	従業員、請負業者、およびサードパーティによる重要なシステムへのリモートアクセスでは、暗号化された接続と多要素認証を使用します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.16	管理責任のないユーザーが不正なソフトウェアをインストールするのを防ぐため、管理的、物理的、技術的なコントロールが行われます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.16	管理責任のないユーザーが不正なソフトウェアをインストールするのを防ぐため、管理的、物理的、技術的なコントロールが行われます。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。
D3.PC.Am.B.16	管理責任のないユーザーが不正なソフトウェアをインストールするのを防ぐため、管理的、物理的、技術的なコントロールが行われます。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.16	管理責任のないユーザーが不正なソフトウェアをインストールするのを防ぐため、管理的、物理的、技術的なコントロールが行われます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
D3.PC.Am.B.2	従業員によるシステムおよび機密データへのアクセスにより、職務の分離が可能になります。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.2	従業員によるシステムおよび機密データへのアクセスにより、職務の分離が可能になります。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
D3.PC.Am.B.2	従業員によるシステムおよび機密データへのアクセスにより、職務の分離が可能になります。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.3	昇格された特権 (例: 管理者権限) は制限され、厳重に制御されます (例: 個人に割り当てられた、共有されないより強力なパスワード制御が必要です)。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.3	昇格された特権 (例: 管理者権限) は制限され、厳重に制御されます (例: 個人に割り当てられた、共有されないより強力なパスワード制御が必要です)。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.3	昇格された特権 (例: 管理者権限) は制限され、厳重に制御されます (例: 個人に割り当てられた、共有されないより強力なパスワード制御が必要です)。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.3	昇格された特権 (例: 管理者権限) は制限され、厳重に制御されます (例: 個人に割り当てられた、共有されないより強力なパスワード制御が必要です)。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.3	昇格された特権 (例: 管理者権限) は制限され、厳重に制御されます (例: 個人に割り当てられた、共有されないより強力なパスワード制御が必要です)。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
D3.PC.Am.B.3	昇格された特権 (例: 管理者権限) は制限され、厳重に制御されます (例: 個人に割り当てられた、共有されないより強力なパスワード制御が必要です)。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
D3.PC.Am.B.6	システム、アプリケーション、ハードウェアへのアクセスには身分証明書と認証を必要とし、それによって管理されます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Am.B.7	アクセスコントロールには、パスワードの複雑さや、パスワードの試行と再利用の制限が含まれます。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
D3.PC.Am.B.8	すべてのデフォルトパスワードと不要なデフォルトアカウントは、システムの実装前に変更されます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.1	ネットワークの境界を防御するツール (例: 境界ルーターやファイアウォール) が使用されています。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.2	インターネットまたは外部からアクセスされるシステムは、ファイアウォールまたはその他の同様のデバイスによって保護されています。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.2	インターネットまたは外部からアクセスされるシステムは、ファイアウォールまたはその他の同様のデバイスによって保護されています。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.2	インターネットまたは外部からアクセスされるシステムは、ファイアウォールまたはその他の同様のデバイスによって保護されています。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.2	インターネットまたは外部からアクセスされるシステムは、ファイアウォールまたはその他の同様のデバイスによって保護されています。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.2	インターネットまたは外部からアクセスされるシステムは、ファイアウォールまたはその他の同様のデバイスによって保護されています。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.2	インターネットまたは外部からアクセスされるシステムは、ファイアウォールまたはその他の同様のデバイスによって保護されています。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.3	すべてのポートがモニタリングされます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
D3.PC.IM.B.3	すべてのポートがモニタリングされます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.3	すべてのポートがモニタリングされます。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
D3.PC.IM.B.3	すべてのポートがモニタリングされます。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.3	すべてのポートがモニタリングされます。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.3	すべてのポートがモニタリングされます。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.5	システム設定 (サーバ、デスクトップ、ルータなど) は業界標準に準拠し、適用されます。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.5	システム設定 (サーバ、デスクトップ、ルータなど) は業界標準に準拠し、適用されます。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.5	システム設定 (サーバ、デスクトップ、ルータなど) は業界標準に準拠し、適用されます。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.6	ポート、機能、プロトコル、サービスは、ビジネス上の目的で不要になった場合には禁止されています。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.6	ポート、機能、プロトコル、サービスは、ビジネス上の目的で不要になった場合には禁止されています。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.6	ポート、機能、プロトコル、サービスは、ビジネス上の目的で不要になった場合には禁止されています。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.IM.B.6	ポート、機能、プロトコル、サービスは、ビジネス上の目的で不要になった場合には禁止されています。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.7	システム設定 (仮想マシンとハイパーバイザーを含む) への変更を行うためのアクセスがコントロールおよびモニタリングされます。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
D3.PC.Im.B.7	システム設定 (仮想マシンとハイパーバイザーを含む) への変更を行うためのアクセスがコントロールおよびモニタリングされます。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.7	システム設定 (仮想マシンとハイパーバイザーを含む) への変更を行うためのアクセスがコントロールおよびモニタリングされます。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.7	システム設定 (仮想マシンとハイパーバイザーを含む) への変更を行うためのアクセスがコントロールおよびモニタリングされます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.7	システム設定 (仮想マシンとハイパーバイザーを含む) への変更を行うためのアクセスがコントロールおよびモニタリングされます。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
D3.PC.Im.B.7	システム設定 (仮想マシンとハイパーバイザーを含む) への変更を行うためのアクセスがコントロールおよびモニタリングされます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Im.B.7	システム設定 (仮想マシンとハイパーバイザーを含む) への変更を行うためのアクセスがコントロールおよびモニタリングされます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
D3.PC.Se.B.1	公共施設で働くデベロッパーは、業界標準を満たすシステム開発ライフサイクル (SDLC) の一部としての、安全なプログラムコーディング慣行に従います。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D3.PC.Se.B.1	公共施設で働くデベロッパーは、業界標準を満たすシステム開発ライフサイクル (SDLC) の一部としての、安全なプログラムコーディング慣行に従います。	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D4.C.Co.B.2	公共施設は、サードパーティーとの接続が許可されていることを確認します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D4.C.Co.B.2	公共施設は、サードパーティーとの接続が許可されていることを確認します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D4.C.Co.B.2	公共施設は、サードパーティーとの接続が許可されていることを確認します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D4.C.Co.B.2	公共施設は、サードパーティーとの接続が許可されていることを確認します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.1	アラート通知パラメータは、緩和アクションを促す情報セキュリティインシデントを検出するために設定されます。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.1	アラート通知パラメータは、緩和アクションを促す情報セキュリティインシデントを検出するために設定されます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.1	アラート通知パラメータは、緩和アクションを促す情報セキュリティインシデントを検出するために設定されます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
D5.DR.De.B.2	システムのパフォーマンスレポートには、情報セキュリティのインシデントを検出するためのリスク指標として使用できる情報が含まれています	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.2	システムのパフォーマンスレポートには、情報セキュリティのインシデントを検出するためのリスク指標として使用できる情報が含まれています	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.DR.De.B.3	インシデント対応プログラムを検出、警告、トリガーするためのツールとプロセスが用意されています。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.ER.Es.B.4	インシデントが分類、記録、追跡されます。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
D5.IR.Pl.B.1	教育機関は、サイバーインシデントにどのように対処し、対応するかを文書化してます。	response-plan-exists-maintained (process check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D5.IR.PI.B.6	公共施設は、ビジネス継続性、災害対策、およびデータバックアッププログラムを使用した、インシデント発生後のオペレーションの復旧を計画します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for FFIEC」で入手できます。

ドイツのクラウドコンピューティングコンプライアンス条件カタログ (C5) の運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレート

としてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、ドイツのクラウドコンピューティングコンプライアンス基準カタログ (C5) と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上のドイツの C5 コントロールに関連付けられます。Germany C5 によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	AWS 設定ルール	ガイダンス
COS-01	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
COS-01	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF

コントロール ID	AWS 設定ルール	ガイダンス
		のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
COS-01	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。
COS-01	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。
COS-01	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。

コントロール ID	AWS 設定ルール	ガイダンス
COS-01	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
COS-03	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
COS-03	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
COS-03	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
COS-03	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
COS-03	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
COS-03	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
COS-03	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
COS-03	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
COS-03	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
COS-03	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
COS-03	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
COS-05	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
COS-05	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
COS-05	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
COS-05	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
COS-05	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
COS-05	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
COS-05	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
COS-05	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
COS-05	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
COS-05	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7
COS-05	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
COS-05	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
COS-05	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-02	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CRY-02	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-02	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号 という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反映する必要があります。
CRY-02	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-02	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CRY-02	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CRY-02	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-02	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CRY-02	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CRY-03	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-03	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
CRY-03	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
CRY-03	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
CRY-03	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-03	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
CRY-03	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CRY-03	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-03	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
CRY-03	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
CRY-03	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
CRY-03	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-03	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CRY-03	codebuild-project-artifact-encryption	保管中の機密データを保護するために、 AWS CodeBuild アーティファクトに対して暗号化が有効になっていることを確認します。
CRY-03	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-03	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
CRY-03	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-03	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CRY-03	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CRY-03	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-04	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。
DEV-07	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
DEV-07	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	AWS 設定ルール	ガイダンス
DEV-07	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
DEV-07	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
DEV-07	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
DEV-07	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
IDM-01	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
IDM-01	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
IDM-01	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
IDM-01	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager シークレットのローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
IDM-01	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
IDM-01	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。
IDM-01	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
IDM-01	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。
IDM-01	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-01	rds-instance-iam-authentication-enabled	システムおよびアセットへのアクセスを制御するために、Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。これにより、データベースに出入りするネットワークトラフィックが、Secure Sockets Layer (SSL) を使用して暗号化されるようになります。認証は外部で管理されるため、ユーザー認証情報をデータベースに保存する必要はありません。
IDM-01	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、 AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-03	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。
IDM-03	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-08	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
CRY-01	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-09	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
IDM-09	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
IDM-09	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
IDM-09	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-01	clb-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。
OPS-01	elbv2-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。
OPS-01	lambda-vpc-multi-az-check	AWS Lambda 関数がアカウントの Virtual Private Cloud (VPC) に接続するように設定されている場合は、Lambda AWS 関数を少なくとも 2 つの異なるアベイラビリティーゾーンにデプロイして、単一のゾーンでサービスが中断された場合に関数がイベントを処理できるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-01	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-01	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-01	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
OPS-01	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-01	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-02	clb-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。
OPS-02	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-02	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
OPS-02	elbv2-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-02	lambda-vpc-multi-az-check	AWS Lambda 関数がアカウントの Virtual Private Cloud (VPC) に接続するように設定されている場合は、Lambda AWS 関数を少なくとも 2 つの異なるアベイラビリティーゾーンにデプロイして、単一のゾーンでサービスが中断された場合に関数がイベントを処理できるようにします。
OPS-02	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-02	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-02	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
OPS-02	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-02	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-07	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-07	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要件を反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-07	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
OPS-07	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
OPS-07	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) では、高可用性と耐障害性のために少なくとも 3 つのデータノードが必要です。少なくとも 3 つのデータノードを持つ OpenSearch Service ドメインをデプロイすると、ノードに障害が発生した場合のクラスターオペレーションが確実になります。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-07	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定:35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。
OPS-07	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-07	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
OPS-07	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-07	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
OPS-07	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-07	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
OPS-07	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-07	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
OPS-07	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-12	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
OPS-12	s3-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
OPS-13	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-13	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-13	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-14	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
OPS-14	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-14	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
OPS-14	s3-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
OPS-15	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-15	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
OPS-15	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
OPS-15	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-15	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
OPS-15	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、Open Search へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-15	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
OPS-15	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
OPS-15	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-15	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
OPS-15	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-15	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
OPS-15	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-15	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
OPS-15	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
OPS-15	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
OPS-22	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

コントロール ID	AWS 設定ルール	ガイダンス
PSS-05	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
PSS-05	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
PSS-05	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
PSS-05	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
PSS-07	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

テンプレート

テンプレートは、GitHub:「ドイツのクラウドコンピューティングコンプライアンス条件カタログ (C5) 運用上のベストプラクティス」で入手できます。

グラムリーチブライリー法 (GLBA) に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

グラムリーチブライリー法 (GLBA) と AWS 管理の Config ルールのマッピングの例を次に示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の GLBA コントロールに関連付けられます。GLBA によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進する	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない		元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(1)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(1) 顧客の記録および情報のセキュリティと機密性を確保する。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(2)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(2) それらの記録のセキュリティまたは完全性に対する予測される脅威または危険から保護する。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(2)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(2) それらの記録のセキュリティまたは完全性に対する予測される脅威または危険から保護する。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
GLBA-SEC.501(b)(3)	サブセクション (a) のポリシーを推進するために、セクション 505(a) に記載されている各機関または当局は、次の各項の目的を達するため、管理上、技術上、および物理的な保護に関して、管轄権の対象となる金融機関に適切な基準を確立しなければならない。(3) 顧客に多大な危害または問題を生じさせる恐れがあるそれらの記録または情報に対する不正なアクセスまたは使用から保護する。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

テンプレート

GitHub から Operational-Best-Practices-for-Gramm-Leach-Bliley-Act.yaml のテンプレートを入手できます。

GxP EU Annex 11 に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

GxP EU Annex 11 と AWS マネージド Config ルール間のマッピングの例を次に示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の GxP EU Annex 11 コントロールに関連付けられます。GxP EU Annex 11 によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1. リスク管理	リスク管理は、患者の安全性、データの完全性、製品の品質を考慮して、コンピュータ化されたシステムのライフサイクル全体に適用する必要があります。リスク管理システムの一部として、検証の範囲とデータ完全性管理に関する決定は、コンピュータ化されたシステムの正当化され文書化されたリスク評価に基づいている必要があります。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
1. リスク管理	リスク管理は、患者の安全性、データの完全性、製品の品質を考慮して、コンピュータ化されたシステムのライフサイクル全体に適用する必要があります。リスク管理システムの一部として、検証の範	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	囲とデータ完全性管理に関する決定は、コンピュータ化されたシステムの正当化され文書化されたリスク評価に基づいている必要があります。		果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
4.2。検証 - ドキュメント変更管理	検証ドキュメントには、変更管理記録 (該当する場合) と検証プロセス中に観察された逸脱に関するレポートを含める必要があります。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.3。確認 - インベントリ	関連するすべてのシステムとその GMP 機能の最新リスト (インベントリ) が用意されている必要があります。重要なシステムについては、物理的および論理的な配置、他のシステムまたはプロセスとのデータフローおよびインターフェイス、ハードウェアおよびソフトウェアの前提条件、およびセキュリティ対策を詳述した最新のシステム記述を用意する必要があります。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.3。確認 - インベントリ	関連するすべてのシステムとその GMP 機能の最新リスト (インベントリ) が用意されている必要があります。重要なシステムについては、物理的および論理的な配置、他のシステムまたはプロセスとのデータフローおよびインターフェイス、ハードウェアおよびソフトウェアの前提条件、およびセキュリティ対策を詳述した最新のシステム記述を用意する必要があります。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.3。確認 - インベントリ	関連するすべてのシステムとその GMP 機能の最新リスト (インベントリ) が用意されている必要があります。重要なシステムについては、物理的および論理的な配置、他のシステムまたはプロセスとのデータフローおよびインターフェイス、ハードウェアおよびソフトウェアの前提条件、およびセキュリティ対策を詳述した最新のシステム記述を用意する必要があります。	ec2-security-group-attached-to-eni-periodic	アセットインベントリを管理するために、このルールでは、セキュリティグループが Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは Elastic Network Interface にアタッチされているかどうかをチェックします。セキュリティグループがこれらのリソースタイプにアタッチされていない場合、それらは使用されていなくて不要である可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.3。確認 - インベントリ	関連するすべてのシステムとその GMP 機能の最新リスト (インベントリ) が用意されている必要があります。重要なシステムについては、物理的および論理的な配置、他のシステムまたはプロセスとのデータフローおよびインターフェイス、ハードウェアおよびソフトウェアの前提条件、およびセキュリティ対策を詳述した最新のシステム記述を用意する必要があります。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.3。確認 - インベントリ	関連するすべてのシステムとその GMP 機能の最新リスト (インベントリ) が用意されている必要があります。重要なシステムについては、物理的および論理的な配置、他のシステムまたはプロセスとのデータフローおよびインターフェイス、ハードウェアおよびソフトウェアの前提条件、およびセキュリティ対策を詳述した最新のシステム記述を用意する必要があります。	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.3。確認 - インベントリ	関連するすべてのシステムとその GMP 機能の最新リスト (インベントリ) が用意されている必要があります。重要なシステムについては、物理的および論理的な配置、他のシステムまたはプロセスとのデータフローおよびインターフェイス、ハードウェアおよびソフトウェアの前提条件、およびセキュリティ対策を詳述した最新のシステム記述を用意する必要があります。	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.8。検証 - データ転送	データが別のデータ形式またはシステムに転送される場合、検証には、この移行プロセス中にデータの値や意味が変更されていないことのチェックを含める必要があります。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. [データ]	他のシステムと電子的にデータを交換するコンピュータ化されたシステムには、リスクを最小限に抑えるために、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要があります。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
7.1。データストレージ - 破損から保護	データは、物理的手段と電子的手段の両方で破損から保護する必要があります。保存されたデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。データへのアクセスは、保管期間を通じて確保する必要があります。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2。データストレージ - バックアップ	すべての関連データの定期的なバックアップを行う必要があります。バックアップデータの完全性と正確性、およびデータの復元が可能であることは、検証中にチェックし、定期的にモニタリングする必要があります。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 監査証跡	リスク評価に基づいて、すべての GMP 関連の変更と削除 (システム生成された「監査証跡」) の記録の作成をシステムに組み込むことを考慮する必要があります。GMP 関連データの変更または削除については、その理由を文書化する必要があります。監査証跡は、利用可能で、一般的にわかりやすい形式に変換可能で、定期的にレビューされる必要があります。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
10. 変更と構成管理	システム構成を含むコンピュータ化されたシステムへの変更は、定義された手順に従って管理された方法でのみ行う必要があります。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. 変更と構成管理	システム構成を含むコンピュータ化されたシステムへの変更は、定義された手順に従って管理された方法でのみ行う必要があります。	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
10. 変更と構成管理	システム構成を含むコンピュータ化されたシステムへの変更は、定義された手順に従って管理された方法でのみ行う必要があります。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 定期的評価	コンピュータ化されたシステムは、有効な状態を維持していて、GMP に準拠していることを確認するために、定期的に評価する必要があります。そのような評価には、必要に応じて、現在の機能範囲、逸脱記録、インシデント、問題、アップグレード履歴、パフォーマンス、信頼性、セキュリティ、および検証についてのステータスレポートを含める必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	rds-instance-iam-authentication-enabled	システムとアセットへのアクセスを制御するために、Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。これにより、データベースに出入りするネットワークトラフィックが、Secure Sockets Layer (SSL) を使用して暗号化されるようになります。認証は外部で管理されるため、ユーザー認証情報をデータベースに保存する必要はありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.1。セキュリティ - 権限者	コンピュータ化されたシステムへのアクセスを権限者に制限するために、物理的および/または論理的な制御を実施する必要があります。システムへの不正な侵入を防ぐには、キー、パスカード、パスワード付きの個人コード、生体認証の使用や、コンピュータ機器およびデータ保存エリアへのアクセス制限などが適切です。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.3。セキュリティ - 認可監査証跡	アクセス認可の作成、変更、キャンセルは記録する必要があります。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.4。セキュリティ - 監査証跡	データおよびドキュメントの管理システムは、データを入力、変更、確認、または削除したオペレータが誰であるかを、日付と時刻とともに記録するように設計する必要があります。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13. インシデント管理	システム障害やデータエラーだけでなく、すべてのインシデントを報告し、評価する必要があります。重大なインシデントの根本原因を特定し、是正処置と予防処置の基礎を形成する必要があります。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13. インシデント管理	システム障害やデータエラーだけでなく、すべてのインシデントを報告し、評価する必要があります。重大なインシデントの根本原因を特定し、是正処置と予防処置の基礎を形成する必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	elbv2-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	lambda-vpc-multi-az-check	AWS Lambda 関数がアカウントの Virtual Private Cloud (VPC) に接続するように設定されている場合は、Lambda AWS 関数を少なくとも 2 つの異なるアベイラビリティーゾーンにデプロイして、単一のゾーンでサービスが中断された場合に関数がイベントを処理できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) では、高可用性と耐障害性のために少なくとも 3 つのデータノードが必要です。少なくとも 3 つのデータノードを持つ OpenSearch Service ドメインをデプロイすると、ノードに障害が発生した場合のクラスターオペレーションが確実になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) クラスターでは、マルチ AZ レプリケーションを有効にして、格納されるデータの可用性をサポートする必要があります。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
16. ビジネス継続性	重要なプロセスをサポートするコンピュータ化されたシステムの可用性については、システムが故障した場合、それらのプロセスのサポートの継続性を確保するための準備 (例: 手動または代替システム) を行う必要があります。代替案を使用するために必要な時間は、リスクに基づいており、特定のシステムとサポートしているビジネスプロセスに見合ったものである必要があります。これらの取り決めは、適切に文書化され、テストされる必要があります。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、バックアップリカバリポイントに最小保持期間が設定されていることを確認します AWS 。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
17. アーカイブ	データはアーカイブされる可能性があります。このデータは、アクセス可能か、読み取り可能か、正確かについてチェックする必要があります。システム (例: コンピュータ機器やプログラム) に関連する変更を行う場合は、データを取得できるかどうかを確認し、テストする必要があります。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for GxP EU Annex 11」(GxP EU Annex 11 に関する運用上のベストプラクティス) で入手できます。

HIPAA Security の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するよう

には設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、医療保険の相互運用性と説明責任に関する法律 (HIPAA) と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の HIPAA コントロールに関連付けられます。「HIPAA」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックは、Payment Card Industry Qualified Security Assessors (QSAs)、HITRUST Certified Common Security Framework Practitioners (CCSFPs)、およびさまざまな業界フレームワークのガイダンスと評価を提供することを認定されたコンプライアンスプロフェッショナルのチームである AWS Security Assurance Services LLC (AWS SAS) によって検証されました。 AWS SAS プロフェッショナルは、お客様が HIPAA のサブセットに合わせることができるようにこのコンフォーマンスパックを設計しました。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(1)(ii)(A)	(A) リスク分析 (必須) 対象となるエンティティが保持する電子的に保護された医療情報の機密性、完全性、可用性に対する潜在的なリスクと脆弱性を正確かつ徹底的に評価します。	annual-risk-assessment-performed (Process Check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性が

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			あるため、転送中の暗号化を有効にしてデータを保護します。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(1)(ii)(B)	(B) リスク管理 (必須)。セクション 164.306(a) に準拠するために、リスクと脆弱性を合理的かつ適切なレベルまで軽減するのに十分なセキュリティ対策を実施します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(i)	(3)(i) 標準: 労働力のセキュリティ 本セクションの (a)(4) 項に規定されているように、全従業員が電子的に保護された医療情報への適切なアクセスを確保し、本セクションの (a)(4) 項に基づき、アクセス権のない全従業員が電子的に保護された医療情報にアクセスすることを防止するためのポリシーと手順を実装します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(A)	(A) 認可および/または監督 (アドレス指定可能) 電子的に保護された医療情報を扱う全従業員またはアクセス可能な場所で作業する全従業員の認可および監督のための手順を実装します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(3)(ii)(B)	(B) 労働力を整理する手順 (アドレス指定可能) 電子的に保護された医療情報への全従業員のアクセスが適切であることを確認する手順を実装します。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(3)(ii)(C)	(C) 終了の手順 (対応方法選択可能)。担当者が退職したとき、またはこのセクションのパラグラフ (a)(3)(ii)(B) の規定による決定に応じて、電子的な保護対象保健情報へのアクセスを終了する手順を実施します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(i)	(4)(i) 標準: 情報へのアクセス管理 このパートのサブパート E の該当する要件と一致する、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(A)	(A) ヘルスケアのクリアリングハウス機能の分離 (必須) ヘルスケアのクリアリングハウスが大規模な組織の一部である場合、クリアリングハウスでは、クリアリングハウスの電子的に保護された医療情報を、大規模な組織による不正アクセスから保護するためのポリシーと手順を実施する必要があります。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(B)	(B) アクセス認可 (アドレス指定可能) ワークステーション、トランザクション、プログラム、プロセス、またはその他のメカニズムへのアクセスを介して、電子的に保護された医療情報へのアクセスを許可するためのポリシーと手順を実装します。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(4)(ii)(C)	(C) アクセスの確立と変更 (アドレス指定可能) エンティティのアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスへのユーザーのアクセス権を確立、ドキュメント化、確認、および変更するポリシーと手順を実装します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(5)(ii)(A)	(A) セキュリティリマインダー (アドレス指定可能) 定期的なセキュリティ更新プログラム	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
164.308 (a)(5)(ii)(A)	(A) セキュリティリマインダー (アドレス指定可能) 定期的なセキュリティ更新プログラム	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(5)(ii)(A)	(A) セキュリティリマインダー (アドレス指定可能) 定期的なセキュリティ更新プログラム	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(5)(ii)(A)	(A) セキュリティリマインダー (アドレス指定可能) 定期的なセキュリティ更新プログラム	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(5)(ii)(B)	(B) 悪意のあるソフトウェアからの保護 (アドレス指定可能) 悪意のあるソフトウェアに対する防御、検出、および報告の手順です。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(5)(ii)(B)	(B) 悪意のあるソフトウェアからの保護 (アドレス指定可能) 悪意のあるソフトウェアに対する防御、検出、および報告の手順です。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(5)(ii)(B)	(B) 悪意のあるソフトウェアからの保護 (アドレス指定可能) 悪意のあるソフトウェアに対する防御、検出、および報告の手順です。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
164.308 (a)(5)(ii)(C)	(C) ログインのモニタリング (アドレス指定可能) ログインの試行をモニタリングし、不一致を報告する手順です。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(5)(ii)(C)	(C) ログインのモニタリング (アドレス指定可能) ログインの試行をモニタリングし、不一致を報告する手順です。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
164.308 (a)(5)(ii)(C)	(C) ログインのモニタリング (アドレス指定可能) ログインの試行をモニタリングし、不一致を報告する手順です。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(5)(ii)(D)	(D) パスワード管理 (アドレス指定可能) パスワードの作成、変更、および保護の手順です。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(6)(i)	(6)(i) 標準: セキュリティインシデントの手順 セキュリティインシデントに対処するためのポリシーと手順を実装します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(6)(ii)	(ii) 実装仕様: 対応と報告 (必須) 疑わしいまたは既知のセキュリティインシデントを特定して対応し、対象となるエンティティに知られているセキュリティインシデントの実用可能な範囲で有害な影響を軽減し、セキュリティインシデントとその結果を文書化します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(i)	(7)(i) 標準: 緊急時対応計画 電子的に保護された医療情報を含むシステムに損害を与える緊急事態またはその他の出来事 (火災、破壊行為、システム障害、自然災害など) に対応するためのポリシーと手順を確立し、必要に応じて実装します。	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(A)	(A) データのバックアップ計画 (必須) 電子的に保護された医療情報の正確なコピーを作成して維持するための手順を確立し、実装します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(B)	(B) 災害対策計画 (必須) データ損失からの復旧のための手順を確立し、必要に応じて実装します。	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(C)	(C) 緊急時のオペレーション計画 (必須) 緊急時の運用において、電子的に保護された医療情報のセキュリティを保護するための重要なビジネスプロセスの継続を可能にする手順を確立し、必要に応じて実装します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(C)	(C) 緊急時のオペレーション計画 (必須) 緊急時の運用において、電子的に保護された医療情報のセキュリティを保護するための重要なビジネスプロセスの継続を可能にする手順を確立し、必要に応じて実装します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
164.308 (a)(7)(ii)(C)	(C) 緊急時のオペレーション計画 (必須) 緊急時の運用において、電子的に保護された医療情報のセキュリティを保護するための重要なビジネスプロセスの継続を可能にする手順を確立し、必要に応じて実装します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(C)	(C) 緊急時のオペレーション計画 (必須) 緊急時の運用において、電子的に保護された医療情報のセキュリティを保護するための重要なビジネスプロセスの継続を可能にする手順を確立し、必要に応じて実装します。	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308 (a)(7)(ii)(C)	(C) 緊急時のオペレーション計画 (必須) 緊急時の運用において、電子的に保護された医療情報のセキュリティを保護するための重要なビジネスプロセスの継続を可能にする手順を確立し、必要に応じて実装します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
164.308 (a)(7)(ii)(C)	(C) 緊急時のオペレーション計画 (必須) 緊急時の運用において、電子的に保護された医療情報のセキュリティを保護するための重要なビジネスプロセスの継続を可能にする手順を確立し、必要に応じて実装します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(8)	(8) 標準: 評価 当初はこのルールに基づいて実装された標準に基づいて、その後、電子的な保護対象保健情報のセキュリティに影響を与える環境または運用の変化に応じて、定期的に技術的および非技術的評価を実施し、エンティティのセキュリティポリシーと手順がこのサブパートの要件をどの程度満たしているかを確定します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.308(a)(8)	(8) 標準: 評価 当初はこのルールに基づいて実装された標準に基づいて、その後、電子的な保護対象保健情報のセキュリティに影響を与える環境または運用の変化に応じて、定期的に技術的および非技術的評価を実施し、エンティティのセキュリティポリシーと手順がこのサブパートの要件をどの程度満たしているかを確定します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール 164.308 (a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的に保護された医療情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(1)	(a)(1) 標準: アクセスコントロール § 164.308(a)(4) の規定に従って、アクセス権限を付与された個人またはソフトウェアプログラムにのみアクセスを許可するための、電子的な保護対象保健情報を維持する電子情報システムの技術的なポリシーと手順を実装します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(i)	(2) 実装仕様: (i) 一意のユーザー ID (必須)。ユーザー ID を識別し追跡するため、一意の名前または番号を割り当てます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
164.312(a)(2)(ii)	(ii) 緊急アクセス手順 (必須) 緊急時に必要な電子的な保護対象保健情報を取得する手順を確立し、必要に応じて実装します。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (a)(2)(iv)	(iv) 暗号化と復号 (アドレス指定可能) 電子的に保護された医療情報を暗号化および復号化するメカニズムを実装します。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	s3-event-notifications-enabled	Amazon S3 イベント通知により、バケットオブジェクトに対する偶発的または意図的な変更について、関連する担当者に警告できます。アラートの例としては、新しいオブジェクトの作成、オブジェクトの削除、オブジェクトの復元、オブジェクトの紛失およびレプリケートなどが含まれます。
164.312 (b)	(b) 標準: 監査のコントロール 電子的に保護された医療情報を含む、または使用する情報システムにおけるアクティビティを記録および調査するハードウェア、ソフトウェア、または手続き型メカニズムを実装します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (c)(1)	(c)(1) 標準: 完全性 電子的に保護された医療情報を、不適切な改ざんや破壊から保護するためのポリシーと手順を実装します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (c)(1)	(c)(1) 標準: 完全性 電子的に保護された医療情報を、不適切な改ざんや破壊から保護するためのポリシーと手順を実装します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (c)(1)	(c)(1) 標準: 完全性 電子的に保護された医療情報を、不適切な改ざんや破壊から保護するためのポリシーと手順を実装します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (c)(1)	(c)(1) 標準: 完全性 電子的に保護された医療情報を、不適切な改ざんや破壊から保護するためのポリシーと手順を実装します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
164.312 (c)(1)	(c)(1) 標準: 完全性 電子的に保護された医療情報を、不適切な改ざんや破壊から保護するためのポリシーと手順を実装します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (c)(2)	(2) 実装仕様: 電子的に保護された医療情報を認証するメカニズム (アドレス指定可能) 電子的に保護された医療情報が、不正な方法で改ざんまたは破壊されていないことを証明する電子的メカニズムを実装します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (c)(2)	(2) 実装仕様: 電子的に保護された医療情報を認証するメカニズム (アドレス指定可能) 電子的に保護された医療情報が、不正な方法で改ざんまたは破壊されていないことを証明する電子的メカニズムを実装します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
164.312 (c)(2)	(2) 実装仕様: 電子的に保護された医療情報を認証するメカニズム (アドレス指定可能) 電子的に保護された医療情報が、不正な方法で改ざんまたは破壊されていないことを証明する電子的メカニズムを実装します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (c)(2)	(2) 実装仕様: 電子的に保護された医療情報を認証するメカニズム (アドレス指定可能) 電子的に保護された医療情報が、不正な方法で改ざんまたは破壊されていないことを証明する電子的メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (c)(2)	(2) 実装仕様: 電子的に保護された医療情報を認証するメカニズム (アドレス指定可能) 電子的に保護された医療情報が、不正な方法で改ざんまたは破壊されていないことを証明する電子的メカニズムを実装します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (d)	(d) 標準: 個人またはエンティティの認証電子的に保護された健康情報へのアクセスを求めている個人またはエンティティが、主張されるとおりのものであることを確認する手順を実装します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
164.312 (d)	(d) 標準: 個人またはエンティティの認証電子的に保護された健康情報へのアクセスを求めている個人またはエンティティが、主張されるとおりのものであることを確認する手順を実装します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (d)	(d) 標準: 個人またはエンティティの認証電子的に保護された健康情報へのアクセスを求めている個人またはエンティティが、主張されるとおりのものであることを確認する手順を実装します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (d)	(d) 標準: 個人またはエンティティの認証電子的に保護された健康情報へのアクセスを求めている個人またはエンティティが、主張されるとおりのものであることを確認する手順を実装します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (d)	(d) 標準: 個人またはエンティティの認証 電子的に保護された健康情報へのアクセスを求めている個人またはエンティティが、主張されるとおりのものであることを確認する手順を実装します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(1)	(e)(1) 標準: 転送のセキュリティ 電子的な通信ネットワークを介して転送される電子的に保護された医療情報を、不正アクセスから保護するための技術的なセキュリティ対策を実装します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(i)	(i) 完全性の管理 (アドレス指定可能) 電子的に送信される電子的に保護された医療情報が、破棄されるまで、発見され不適切に変更されないようにするためのセキュリティ対策を実装します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
164.312 (e)(2)(ii)	(ii) 暗号化 (アドレス指定可能) 電子的に保護された医療情報が、適切と判断された場合に必ず暗号化されるメカニズムを実装します。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(1)	(b)(1) 標準: グループ健康保険の要件 保険の管理者に開示された唯一の電子的な保護対象保健情報が § 164.504(f)(1)(ii) または (iii) に従って開示されている場合、または § 164.508 で許可されているために開示されている場合を除き、グループ健康保険では、グループ健康保険の業務として保険の管理者によって作成、受領、維持、送信、または受信された電子的な保護対象保健情報を保険の管理者が合理的かつ適切に保護することを、保険のドキュメントに必ず規定する必要があります。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。(ii) § 164.504(f)(2)(iii) によって要求される適切な分離が、合理的かつ適切なセキュリティ対策によってサポートされていることを確認する。(iii) この情報が提供されるすべてのエージェント (下請業者を含む) が、情報を保護するための合理的かつ適切なセキュリティ対策を実施することに同意していることを	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	確認する。(iv) セキュリティインシデントに気付いた場合は、グループ健康保険に報告する。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。(AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			映する必要があります。
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
164.314(b)(2)(i)	(2) 実装仕様 (必須) グループ健康保険の保険ドキュメントは、保険の管理者に次のことを要求する規定を組み込むように修正する必要があります。(i) 保険の管理者がグループ健康保険の業務として作成、受領、維持、または送信する電子的な保護対象保健情報の機密性、完全性、および可用性を合理的かつ適切に保護する管理的、物理的、および技術的な保護手段を実施する。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for HIPAA Security」で入手できます。

IRS 1075 に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、IRS 1075 と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の IRS 1075 コントロールに関連付けられま

す。IRS 1075 によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング d。転送時のデータ暗号化	FTI はクラウド環境内で転送中に暗号化する必要があります。FTI の暗号化に使用されるすべてのメカニズムは FIPS 140 認定を受けており、最新の FIPS 140 準拠モジュールを利用して動作する必要があります。この要件は SLA に含める必要があります。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.3.1 クラウドコンピューティング d。転送時のデータ暗号化	FTI はクラウド環境内で転送中に暗号化する必要があります。FTI の暗号化に使用されるすべてのメカニズムは FIPS 140 認定を受けており、最新の FIPS 140 準拠モジュールを利用して動作する必要があります。この要件は SLA に含める必要があります。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング d。転送時のデータ暗号化	FTI はクラウド環境内で転送中に暗号化する必要があります。FTI の暗号化に使用されるすべてのメカニズムは FIPS 140 認定を受けており、最新の FIPS 140 準拠モジュールを利用して動作する必要があります。この要件は SLA に含める必要があります。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.3.1 クラウドコンピューティング d。転送時のデータ暗号化	FTI はクラウド環境内で転送中に暗号化する必要があります。FTI の暗号化に使用されるすべてのメカニズムは FIPS 140 認定を受けており、最新の FIPS 140 準拠モジュールを利用して動作する必要があります。この要件は SLA に含める必要があります。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング d。転送時のデータ暗号化	FTI はクラウド環境内で転送中に暗号化する必要があります。FTI の暗号化に使用されるすべてのメカニズムは FIPS 140 認定を受けており、最新の FIPS 140 準拠モジュールを利用して動作する必要があります。この要件は SLA に含める必要があります。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.3.1 クラウドコンピューティング d。転送時のデータ暗号化	FTI はクラウド環境内で転送中に暗号化する必要があります。FTI の暗号化に使用されるすべてのメカニズムは FIPS 140 認定を受けており、最新の FIPS 140 準拠モジュールを利用して動作する必要があります。この要件は SLA に含める必要があります。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング d。転送時のデータ暗号化	FTI はクラウド環境内で転送中に暗号化する必要があります。FTI の暗号化に使用されるすべてのメカニズムは FIPS 140 認定を受けており、最新の FIPS 140 準拠モジュールを利用して動作する必要があります。この要件は SLA に含める必要があります。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.3.1 クラウドコンピューティング e。保管時のデータ暗号化	保存時のデータ暗号化である FTI は、クラウドに保存されている間も、最新の FIPS 140 認定を受けた暗号化メカニズムを使用して暗号化する必要があります。この要件は SLA に含める必要があります。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング k。多要素認証	政府機関は、自社のクラウドソリューションがインターネットから利用できる場合 (つまり、政府機関の信頼できるネットワークの外部からクラウドソリューションにアクセスできる場合)、十分な多要素認証を実装する必要があります。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング k。多要素認証	政府機関は、自社のクラウドソリューションがインターネットから利用できる場合 (つまり、政府機関の信頼できるネットワークの外部からクラウドソリューションにアクセスできる場合)、十分な多要素認証を実装する必要があります。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング k。多要素認証	政府機関は、自社のクラウドソリューションがインターネットから利用できる場合 (つまり、政府機関の信頼できるネットワークの外部からクラウドソリューションにアクセスできる場合)、十分な多要素認証を実装する必要があります。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 クラウドコンピューティング k。多要素認証	政府機関は、自社のクラウドソリューションがインターネットから利用できる場合 (つまり、政府機関の信頼できるネットワークの外部からクラウドソリューションにアクセスできる場合)、十分な多要素認証を実装する必要があります。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
3.3.1 クラウドコンピューティング i。IT リスク評価	政府機関は、FTI の受信、処理、保存、アクセス、保護、および/または送信に使用されるすべての情報システムに対して実施されているセキュリティおよびプライバシー管理について、毎年評価を実施する必要があります。	annual-risk-assessment-performed(Process Check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	netfw-policy-rule-group-associated	AWS Network Firewall ポリシーは、ファイアウォールが Amazon VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定して、パケットとトラフィックフローのフィルタリングし、デフォルトのトラフィック処理を定義します。
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	netfw-stateless-rule-group-not-empty	AWS Network Firewall ルールグループには、ファイアウォールが VPC 内のトラフィックを処理する方法を定義するルールが含まれています。ファイアウォールポリシーに空のステートレスルールグループが存在する場合、トラフィックは処理されません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.6 ネットワーク境界とインフラストラクチャ	政府機関は、FTI および FTI システムを保護するために、ルーター、ファイアウォール、スイッチ、侵入検知システムなど、システムアーキテクチャ全体に境界保護デバイスを導入する必要があります。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (f)	機関のアカウント管理手順の前提条件にしたがって、アカウントを作成、有効化、変更、無効化、および削除します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (f)	機関のアカウント管理手順の前提条件にしたがって、アカウントを作成、有効化、変更、無効化、および削除します。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
AC-2 アカウントの管理 (f)	機関のアカウント管理手順の前提条件にしたがって、アカウントを作成、有効化、変更、無効化、および削除します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (f)	機関のアカウント管理手順の前提条件にしたがって、アカウントを作成、有効化、変更、無効化、および削除します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (f)	機関のアカウント管理手順の前提条件にしたがって、アカウントを作成、有効化、変更、無効化、および削除します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (g)	アカウントの使用状況をモニタリングします	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
AC-2 アカウントの管理 (g)	アカウントの使用状況をモニタリングします	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (g)	アカウントの使用状況をモニタリングします	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (g)	アカウントの使用状況をモニタリングします	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AC-2 アカウントの管理 (g)	アカウントの使用状況をモニタリングします	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (g)	アカウントの使用状況をモニタリングします	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (g)	アカウントの使用状況をモニタリングします	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (g)	アカウントの使用状況をモニタリングします	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	secretsmanager-secret-periodic-rotation	このルールにより、 AWS Secrets Manager シークレットで定期的なローテーションが有効になっていることが保証されます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 アカウントの管理 (j)	アカウント管理要件への準拠について、アカウントを確認します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
(CE-1) 自動システムアカウント管理	[Assignment: organization-defined automated mechanisms] (割り当て: 組織で定義された自動化されたメカニズム) を使用して、システムアカウントの管理をサポートします。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
(CE-1) 自動システムアカウント管理	[Assignment: organization-defined automated mechanisms] (割り当て: 組織で定義された自動化されたメカニズム) を使用して、システムアカウントの管理をサポートします。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
(CE-1) 自動システムアカウント管理	[Assignment: organization-defined automated mechanisms] (割り当て: 組織で定義された自動化されたメカニズム) を使用して、システムアカウントの管理をサポートします。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
(CE-3): アカウントの無効化	アカウントが以下の場合は 120 日以内にアカウントを無効にします。a。期限が切れている、b。ユーザーまたは個人に関連付けられなくなった、c。組織の方針に違反している、または d。非特権アカウントでは 120 日間、特権アカウントでは 60 日間非アクティブになっている	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
(CE-12) 非定型使用のアカウントモニタリング	システムアカウントの異常な使用をモニタリングし、システムアカウントの異常な使用について機関で定義された担当者またはロールに報告します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 最小特権	最小特権の原則を採用し、組織に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17: リモートアクセス	許可されているリモートアクセスの種類ごとに、使用制限、構成/接続要件、および実装ガイダンスを確立して文書化し、システムへの各タイプのリモートアクセスを許可してからそれらの接続を許可します。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。
AT-1: 意識向上と訓練	システムユーザー (管理者、上級幹部、請負業者を含む) にセキュリティおよびプライバシーリテラシートレーニングを実施します。	security-awareness-program-exists(Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2: 監査イベント	監査機能をサポートするために、システムがログに記録できるイベントのタイプを特定します	audit-log-policy-exists(Process Check)	組織のログ要件を定義する、監査ログの管理ポリシーを確立して維持します。これには監査ログのレビューと保持が含まれますが、これらに限定されるわけではありません。
AU-16: 組織間の監査ロギング	監査情報が組織の境界を越えて伝達される場合、外部組織間で機関が定義した監査情報を調整する機関が定義した方法を採用します。	audit-log-policy-exists(Process Check)	組織のログ要件を定義する、監査ログの管理ポリシーを確立して維持します。これには監査ログのレビューと保持が含まれますが、これらに限定されるわけではありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7: 継続的なモニタリング	システムレベルの継続的モニタリング戦略の策定、および組織レベルの継続的モニタリング戦略に従った継続的モニタリングの実施。機関が定義したモニタリングする指標の確立。継続的モニタリング戦略に従った継続的なコントロールの評価。継続的モニタリング戦略に従ったシステムおよび組織が定める指標のモニタリング。コントロール評価とモニタリングによって生成された情報の相関と分析。こコントロール評価とモニタリング情報の分析結果に対処するための対応措置。システムのセキュリティおよびプライバシーの状況について少なくとも 1 年に 1 度の頻度で報告。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するために、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9: システムバックアップ	a。セキュリティ関連文書など、システム文書に含まれるユーザーレベルの情報のバックアップを毎週実施します。b。システムに含まれるシステムレベルの情報のバックアップを毎週実施します。c。セキュリティおよびプライバシー関連文書を含むシステム文書のバックアップを毎週実施します。d。バックアップ情報の機密性、完全性、可用性を保護します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2: 身分証明書と認証 (組織のユーザー) (CE-1) 特権アカウントへの多要素認証	特権アカウントへのアクセスに多要素認証を導入します	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2: 身分証明書と認証 (組織のユーザー) (CE-1) 特権アカウントへの多要素認証	特権アカウントへのアクセスに多要素認証を導入します	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2: 身分証明書と認証 (組織のユーザー) (CE-2) 非特権アカウントへの多要素認証	非特権アカウントへのアクセスに多要素認証を導入します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5: Authenticator の管理: (CE-1) パスワードベースの認証:パスワードベースの認証用	以下の構成と複雑さのルールを適用します。1. パスワードの最小長を 14 文字にします。2. 数字、大文字、小文字、特殊文字を組み合わせたパスワードの複雑さを最小限として加えます。3. 新しいパスワードを使用するときは、少なくとも 1 文字の変更を強制します。4. 暗号で保護されたパスワードのみを保存および転送します。5. パスワードの有効期限の制限を強制します。i。最短 1 日、最長 90 日。ii。サービスアカウントのパスワードは、366 日以内 (含む) に失効します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PM-5: システムインベントリ	組織システムのインベントリを継続的に開発および更新します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PM-5: システムインベントリ	組織システムのインベントリを継続的に開発および更新します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PM-5: システムインベントリ	組織システムのインベントリを継続的に開発および更新します。	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PM-5: システムインベントリ	組織システムのインベントリを継続的に開発および更新します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
RA-5: 脆弱性のモニタリングとスキャン	システムおよびホストされているアプリケーションの脆弱性について、30 日毎、機関のネットワークに新しい情報システムを導入する前、およびシステムに影響を与える可能性のある新たな脆弱性が特定され、報告された場合にモニタリングとスキャンを行います。	vuln-scans-performed(Process Check)	コンプライアンス要件に従って脆弱性スキャンが実行されていることを確認します。スキャンの周期、使用するツール、結果の使用方法については、組織が定義する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10: 開発者設定管理 (e.)	システム、コンポーネント、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10: 開発者設定管理 (e.)	システム、コンポーネント、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10: 開発者設定管理 (e.)	システム、コンポーネント、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-10: 開発者設定管理 (a) (c.)	システム、コンポーネント、サービスの設計、開発、実装、運用の際に設定管理を実行します。システム、コンポーネント、サービスには組織が承認した変更のみを実装します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-4: 共有システムリソース内の情報	共有システムリソースからの、未許可の意図しない情報転送を防止します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界の保護	システムの外部境界およびシステム内の主要な内部境界で通信をモニタリングおよびコントロールします。内部の組織ネットワークから分離されたパブリックアクセス可能なシステムコンポーネント用のサブネットワークを実装します。外部ネットワークや情報システムを、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成されるマネージドインターフェイスのみを通じて接続します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界保護 (CE-9) 脅威となる送信通信トラフィックの制限	(a) 外部システムへの脅威となる送信通信トラフィックを検出して拒否します。拒否された通信に関連する内部ユーザーの ID を監査します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界保護 (CE-9) 脅威となる送信通信トラフィックの制限	(a) 外部システムへの脅威となる送信通信トラフィックを検出して拒否します。拒否された通信に関連する内部ユーザーの ID を監査します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界保護 (CE-9) 脅威となる送信通信トラフィックの制限	(a) 外部システムへの脅威となる送信通信トラフィックを検出して拒否します。拒否された通信に関連する内部ユーザーの ID を監査します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7: 境界保護 (IRS 定義)	政府機関は、信頼境界で境界保護 (通常はファイアウォールを使用) を実施および管理する必要があります。各信頼境界をモニタリングし、各境界を越える通信を制御する必要があります。	netfw-policy-rule-group-associated	AWS Network Firewall ポリシーは、ファイアウォールが Amazon VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定して、パケットとトラフィックフローのフィルタリングし、デフォルトのトラフィック処理を定義します。
SC-7: 境界保護 (IRS 定義)	政府機関は、信頼境界で境界保護 (通常はファイアウォールを使用) を実施および管理する必要があります。各信頼境界をモニタリングし、各境界を越える通信を制御する必要があります。	netfw-stateless-rule-group-not-empty	AWS Network Firewall ルールグループには、ファイアウォールが VPC 内のトラフィックを処理する方法を定義するルールが含まれています。ファイアウォールポリシーに空のステートレスルールグループが存在する場合、トラフィックは処理されません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8: 伝送の機密性と完全性 (CE-1) 暗号化保護	送信時に情報の不正な開示を防止し、情報の変更を検出するに暗号化メカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8: 伝送の機密性と完全性 (CE-1) 暗号化保護	送信時に情報の不正な開示を防止し、情報の変更を検出するに暗号化メカニズムを実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8: 伝送の機密性と完全性 (CE-1) 暗号化保護	送信時に情報の不正な開示を防止し、情報の変更を検出するに暗号化メカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8: 伝送の機密性と完全性 (CE-1) 暗号化保護	送信時に情報の不正な開示を防止し、情報の変更を検出するに暗号化メカニズムを実装します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8: 伝送の機密性と完全性 (CE-1) 暗号化保護	送信時に情報の不正な開示を防止し、情報の変更を検出するに暗号化メカニズムを実装します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8: 伝送の機密性と完全性 (CE-1) 暗号化保護	送信時に情報の不正な開示を防止し、情報の変更を検出するに暗号化メカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8: 伝送の機密性と完全性 (CE-1) 暗号化保護	送信時に情報の不正な開示を防止し、情報の変更を検出するに暗号化メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-12: 暗号化キーの確立と管理	機関は、キーの生成、配布、保存、アクセス、破棄について、キーの管理要件である NIST SP 800-57 (キー管理の推奨事項) に従ってシステムに暗号化を使用する場合、暗号化キーを作成し、管理する必要があります。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12: 暗号化キーの確立と管理	機関は、キーの生成、配布、保存、アクセス、破棄について、キーの管理要件である NIST SP 800-57 (キー管理の推奨事項) に従ってシステムに暗号化を使用する場合、暗号化キーを作成し、管理する必要があります。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13: 暗号化による保護	最新の FIPS-140 で検証された暗号化メカニズム、NIST 800-52、Transport Layer Security (TLS) 実装の選択、設定、および使用のためのガイドライン、転送中の暗号化 (ペイロード暗号化)の中から、指定された各暗号化の用途に必要なタイプの暗号化を実装します。デジタル署名に SHA-1 を使用することは禁止されています。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23: セッションの認証性	通信のセッションの信頼性を確保します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28: 保存中の情報に対する保護 (CE-1) 暗号化による保護	暗号化メカニズムを導入して、不揮発性ストレージ内のエンドユーザーコンピューティングシステム (デスクトップコンピューター、ラップトップコンピューター、モバイルデバイス、ポータブルおよびリムーバブルストレージデバイスなど) に保存されている FTI の不正な開示と変更を防止します。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2: 不具合の修復 (IRS 定義)	政府機関は、毎日ワークステーションの電源を入れて機関のネットワークに接続したときに、(ポリシーで定義されているとおり、GFE ワークステーションを使用するリモート接続を含めて) 機関が承認した最新のパッチが適用されていること、および存在しないパッチまたは新しいパッチが必要に応じて適用されていることについて、ワークステーションがチェックされていることを確認します。また、それ以外の場合は 24 時間に 1 回以上 (土日祝日などを除く) チェックされていることを確認します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2: 不具合の修復 (IRS 定義)	政府機関は、毎日ワークステーションの電源を入れて機関のネットワークに接続したときに、(ポリシーで定義されているとおり、GFE ワークステーションを使用するリモート接続を含めて) 機関が承認した最新のパッチが適用されていること、および存在しないパッチまたは新しいパッチが必要に応じて適用されていることについて、ワークステーションがチェックされていることを確認します。また、それ以外の場合は 24 時間に 1 回以上 (土日祝日などを除く) チェックされていることを確認します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2: 不具合の修復 (IRS 定義)	政府機関は、毎日ワークステーションの電源を入れて機関のネットワークに接続したときに、(ポリシーで定義されているとおり、GFE ワークステーションを使用するリモート接続を含めて) 機関が承認した最新のパッチが適用されていること、および存在しないパッチまたは新しいパッチが必要に応じて適用されていることについて、ワークステーションがチェックされていることを確認します。また、それ以外の場合は 24 時間に 1 回以上 (土日祝日などを除く) チェックされていることを確認します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2: 不具合の修復 (IRS 定義)	政府機関は、毎日ワークステーションの電源を入れて機関のネットワークに接続したときに、(ポリシーで定義されているとおり、GFE ワークステーションを使用するリモート接続を含めて) 機関が承認した最新のパッチが適用されていること、および存在しないパッチまたは新しいパッチが必要に応じて適用されていることについて、ワークステーションがチェックされていることを確認します。また、それ以外の場合は 24 時間に 1 回以上 (土日祝日などを除く) チェックされていることを確認します。	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。 AWS Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 はプラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2: 不具合の修復 (IRS 定義)	政府機関は、毎日ワークステーションの電源を入れて機関のネットワークに接続したときに、(ポリシーで定義されているとおり、GFE ワークステーションを使用するリモート接続を含めて) 機関が承認した最新のパッチが適用されていること、および存在しないパッチまたは新しいパッチが必要に応じて適用されていることについて、ワークステーションがチェックされていることを確認します。また、それ以外の場合は 24 時間に 1 回以上 (土日祝日などを除く) チェックされていることを確認します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2: 不具合の修復 (IRS 定義)	政府機関は、毎日ワークステーションの電源を入れて機関のネットワークに接続したときに、(ポリシーで定義されているとおり、GFE ワークステーションを使用するリモート接続を含めて) 機関が承認した最新のパッチが適用されていること、および存在しないパッチまたは新しいパッチが必要に応じて適用されていることについて、ワークステーションがチェックされていることを確認します。また、それ以外の場合は 24 時間に 1 回以上 (土日祝日などを除く) チェックされていることを確認します。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング	組織: a。情報システムをモニタリングします。1. [Assignment: organization-defined monitoring objective] (割り当て: 組織が定義したモニタリング目標) に従った攻撃と潜在的な攻撃の指標、2. ローカル、ネットワーク、およびリモートへの不正な接続、b。[Assignment: organization-defined techniques and methods] (割り当て: 組織で定義された技術と方法) を通じて、情報システムの不正使用を特定します、1. 組織で決められた必須情報を収集するため、情報システム内に戦略的に配置します、2。組織にとって重要な特定の種類のトランザクションを追跡するための、システム内のアドホックの場所、d. 侵入監視ツールから取得した情報を不正なアクセス、変更、	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	削除から保護します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング	組織: a。情報システムをモニタリングします。1. [Assignment: organization-defined monitoring objective] (割り当て: 組織が定義したモニタリング目標) に従った攻撃と潜在的な攻撃の指標、2. ローカル、ネットワーク、およびリモートへの不正な接続、b。[Assignment: organization-defined techniques and methods] (割り当て: 組織で定義された技術と方法) を通じて、情報システムの不正使用を特定します、1. 組織で決められた必須情報を収集するため、情報システム内に戦略的に配置します、2。組織にとって重要な特定の種類のトランザクションを追跡するための、システム内のアドホックの場所、d. 侵入監視ツールから取得した情報を不正なアクセス、変更、	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	削除から保護します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング	組織: a。情報システムをモニタリングします。1. [Assignment: organization-defined monitoring objective] (割り当て: 組織が定義したモニタリング目標) に従った攻撃と潜在的な攻撃の指標、2. ローカル、ネットワーク、およびリモートへの不正な接続、b。[Assignment: organization-defined techniques and methods] (割り当て: 組織で定義された技術と方法) を通じて、情報システムの不正使用を特定します、1. 組織で決められた必須情報を収集するため、情報システム内に戦略的に配置します、2。組織にとって重要な特定の種類のトランザクションを追跡するための、システム内のアドホックの場所、d. 侵入監視ツールから取得した情報を不正なアクセス、変更、	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	削除から保護します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング	組織: a。情報システムをモニタリングします。1. [Assignment: organization-defined monitoring objective] (割り当て: 組織が定義したモニタリング目標) に従った攻撃と潜在的な攻撃の指標、2. ローカル、ネットワーク、およびリモートへの不正な接続、b。[Assignment: organization-defined techniques and methods] (割り当て: 組織で定義された技術と方法) を通じて、情報システムの不正使用を特定します、1. 組織で決められた必須情報を収集するため、情報システム内に戦略的に配置します、2。組織にとって重要な特定の種類のトランザクションを追跡するための、システム内のアドホックの場所、d. 侵入監視ツールから取得した情報を不正なアクセス、変更、	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	削除から保護します。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング	組織: a。情報システムをモニタリングします。1. [Assignment: organization-defined monitoring objective] (割り当て: 組織が定義したモニタリング目標) に従った攻撃と潜在的な攻撃の指標、2. ローカル、ネットワーク、およびリモートへの不正な接続、b。[Assignment: organization-defined techniques and methods] (割り当て: 組織で定義された技術と方法) を通じて、情報システムの不正使用を特定します、1. 組織で決められた必須情報を収集するため、情報システム内に戦略的に配置します、2。組織にとって重要な特定の種類のトランザクションを追跡するための、システム内のアドホックの場所、d. 侵入監視ツールから取得した情報を不正なアクセス、変更、	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	削除から保護します。		
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4: システムモニタリング (IRS 定義)	すべてのインターネットアクセスポイント/ポータルは、承認されたインターネット「匿名」接続 (CISO 機関の承認などによるもの) を除き、インバウンドおよびアウトバウンドのトラフィックヘッダー情報を少なくとも 1 年間キャプチャし、保持するものとします。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7: ソフトウェア、ファームウェア、および情報の整合性	完全性検証ツールを使用して、システムカーネル、ドライバー、ファームウェア (例: BIOS、UEFI)、ソフトウェア (例: OS、アプリケーション、ミドルウェア) およびセキュリティ属性など、ソフトウェア、ファームウェアおよび情報に対する不正な変更を検出します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7: ソフトウェア、ファームウェア、および情報の整合性	完全性検証ツールを使用して、システムカーネル、ドライバー、ファームウェア (例: BIOS、UEFI)、ソフトウェア (例: OS、アプリケーション、ミドルウェア) およびセキュリティ属性など、ソフトウェア、ファームウェアおよび情報に対する不正な変更を検出します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7: ソフトウェア、ファームウェア、および情報の整合性	完全性検証ツールを使用して、システムカーネル、ドライバー、ファームウェア (例: BIOS、UEFI)、ソフトウェア (例: OS、アプリケーション、ミドルウェア) およびセキュリティ属性など、ソフトウェア、ファームウェアおよび情報に対する不正な変更を検出します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	dynamodb-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するには、Amazon DynamoDB リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	バックアップ計画によって保護された EBS リソース	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) リソースが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	バックアップ計画によって保護された efs リソース	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	rds-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	s3-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12: 情報の管理と保持	組織は、適用される法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、システム内の情報およびシステムから出力される情報を管理および保持します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

テンプレート

テンプレートは、GitHub の「IRS 1075 運用のベストプラクティス」で入手できます。

K-ISMS の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、韓国 - 情報セキュリティ管理システム (ISMS) と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールが特定の AWS リソースに適用され、1 つ以上の韓国の「ISMS」によるコントロールに関連付けられます。韓国の「ISMS」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	AWS 設定ルール	ガイダンス
1.2.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
1.2.1	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
2.1.3	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager

コントロール ID	AWS 設定ルール	ガイダンス
		は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
2.1.3	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
2.3.3	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
2.3.3	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
2.5.1	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.1	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
2.5.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.1	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
2.5.1	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.1	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
2.5.1	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.1	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
2.5.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.1	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
2.5.1	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.1	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2.5.3	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.3	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
2.5.3	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.4	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.5.5	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
2.5.5	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
2.5.5	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。
2.6	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
2.6	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
2.6	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
2.6	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
2.6	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。
2.6	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
2.6	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
2.6	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.6	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
2.6	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
2.6.6	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
2.6.6	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
2.6.6	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.6.6	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
2.6.6	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
2.6.6	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.6.6	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
2.6.6	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.6.6	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
2.6.6	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.6.6	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
2.6.6	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
2.6.7	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
2.7	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
2.7	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
2.7	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.7	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2.7	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
2.7	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
2.7	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
2.7	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2.7	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
2.7	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
2.7	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.7	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
2.7	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.7	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
2.7	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2.7	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
2.7	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
2.7	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
2.7	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
2.7	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.7	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
2.7	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2.7	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2.7	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
2.7	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.7.1	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
2.7.1	elb-predefined-security-policy-ssl-check	転送中のデータを保護するため、Classic Elastic Load Balancing のリスナーがカスタムセキュリティポリシーを使用していることを確認します。Elastic Load Balancing には、クライアントとロードバランサーの間に接続が確立されたときに SSL ネゴシエーションに使用される定義済み SSL ネゴシエーション設定があります。SSL ネゴシエーション設定は幅広いクライアントとの互換性を提供し、暗号 という強力な暗号アルゴリズムを使用します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは ELBSecurityPolicy-TLS-1-2-2017-0 です。実際の値には、組織のポリシーを反映する必要があります。
2.7.2	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
2.7.2	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
2.8.5	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.8.5	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、 AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
2.8.6	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.8.6	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、 AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
2.9.1	account-part-of-organizations	AWS Organizations AWS アカウント 内の の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
2.9.1	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.1	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.2	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.2	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.2	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.2	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
2.9.2	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.2	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。
2.9.3	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.3	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
2.9.3	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.3	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
2.9.3	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.3	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
2.9.3	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.3	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
2.9.3	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.3	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.3	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.3	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
2.9.3	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.3	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
2.9.3	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.3	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
2.9.3	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.4	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
2.9.4	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
2.9.4	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.4	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
2.9.4	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.4	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.4	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
2.9.4	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.4	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
2.9.4	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
2.9.4	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
2.10.3	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.10.3	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
2.10.3	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.10.3	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
2.10.3	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
2.10.5	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
2.10.5	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.10.5	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.10.5	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
2.10.5	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.10.5	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.10.5	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
2.10.5	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.10.8	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.10.8	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
2.11.2	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.11.3	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。
2.11.3	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
2.11.3	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
2.11.3	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
2.11.3	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	AWS 設定ルール	ガイダンス
2.11.3	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
2.12	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
2.12	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
2.12	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
2.12	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
2.12	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。
2.12	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
2.12	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
2.12	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.12	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要件を反映する必要があります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for K-ISMS」で入手できます。

ロードバランシングの運用のベストプラクティス

このコンフォーマンスパックには、内部の負荷分散に基づく AWS Config ルールが含まれています AWS。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Load Balancing」で入手できます。

ログ記録に関する運用上のベストプラクティス

このコンフォーマンスパックには、ログ記録に基づく AWS Config ルールが含まれています AWS。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Logging」で入手できます。

サービスの管理およびガバナンスの運用のベストプラクティス

このコンフォーマンスパックには、 管理およびガバナンスサービスに基づく AWS Config ルールが含まれています。詳細については、「 の管理とガバナンス AWS」を参照してください。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Management and Governance Services」で入手できます。

シンガポール金融管理局の「Notice 655」の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、シンガポール金融管理局 (MAS) 通知 655 – Cyber Hygiene と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上

の MAS Notice 655 – Cyber Hygiene コントロールに関連付けられます。シンガポール金融管理局の「Notice 655 - Cyber Hygiene」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
4.1	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値に

コントロール ID	AWS 設定ルール	ガイダンス
		は、組織のポリシーを反映する必要があります。
4.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
4.1	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
4.1	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
4.1	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。
4.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
4.1	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。
4.1	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
4.1	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.2	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
4.2	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	AWS 設定ルール	ガイダンス
4.2	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
4.2	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.2	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
4.2	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	AWS 設定ルール	ガイダンス
4.2	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
4.2	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

コントロール ID	AWS 設定ルール	ガイダンス
4.3	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
4.3	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
4.3	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
4.3	account-part-of-organizations	AWS Organizations AWS アカウント 内の の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
4.4	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
4.4	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
4.4	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
4.4	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
4.4	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
4.4	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
4.4	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
4.4	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
4.4	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。
4.4	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。
4.4	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーは、ファイアウォールが Amazon VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定し、パケットとトラフィックフローをフィルタリングします。Pass アクションをデフォルトに設定すると、意図しないトラフィックが許可される可能性があります。
4.4	netfw-policy-default-action-full-packets	AWS Network Firewall ポリシーは、ファイアウォールが Amazon VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定し、パケットとトラフィックフローをフィルタリングします。Pass アクションをデフォルトに設定すると、意図しないトラフィックが許可される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	netfw-policy-rule-group-associated	AWS Network Firewall ポリシーは、ファイアウォールが Amazon VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定して、パケットとトラフィックフローのフィルタリングし、デフォルトのトラフィック処理を定義します。
4.4	netfw-stateless-rule-group-not-empty	AWS Network Firewall ルールグループには、ファイアウォールが VPC 内のトラフィックを処理する方法を定義するルールが含まれています。ファイアウォールポリシーに空のステートレスルールグループが存在する場合、トラフィックは処理されません。
4.4	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
4.4	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
4.4	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
4.4	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
4.4	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
4.4	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
4.4	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
4.4	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
4.4	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
4.5	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
4.5	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
4.5	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
4.5	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
4.6	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.6	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
4.6	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
4.6	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
4.6	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
4.6	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for MAS Notice 655」で入手できます。

MAS TRMGの運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下は、シンガポール金融管理局 (MAS) の「Technology Risk Managment Guidelines (TRMG) January 2021」と、 AWS マネージド Config ルール間のマッピングの例です。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の MAS TRMG コントロールに関連付けられます。MAS の「TRMG January 2021」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	AWS 設定ルール	ガイダンス
3.3.1	account-part-of-organizations	AWS Organizations AWS アカウント 内の の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
5.4.3	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
5.4.3	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまた

コントロール ID	AWS 設定ルール	ガイダンス
		はサインイン認証情報ではなく、OAuth を使用します。
6.1.1	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
6.1.2	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
6.1.4	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
6.1.4	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
6.1.4	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
6.2.1	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。
6.3.1	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.5	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
6.4.5	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
6.4.5	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
6.4.5	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.5	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
6.4.5	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
6.4.5	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.5	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
6.4.5	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
6.4.5	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.5	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
6.4.5	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
6.4.6	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.6	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
6.4.6	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.6	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
6.4.6	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.6	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
6.4.6	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.6	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.6	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.6	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
6.4.7	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
6.4.7	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.7	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
6.4.7	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.7	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
6.4.7	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
6.4.7	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.7	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
6.4.7	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.7	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
6.4.7	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.7	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.7	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.7	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
6.4.7	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。 AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.8	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
6.4.8	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.8	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。
6.4.8	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.8	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
6.4.8	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.8	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4.8	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
7.2.1	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
7.2.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
7.4.1	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
7.4.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
7.4.1	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
7.4.1	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。
7.4.1	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	AWS 設定ルール	ガイダンス
7.4.1	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
7.5.5	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.5	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
7.5.5	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.5	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
7.5.5	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.5	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
7.5.5	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.5	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。
7.5.5	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.5	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
7.5.7	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
7.5.7	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.7	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
7.5.7	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
7.5.7	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.7	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
7.5.7	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
7.5.7	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.7	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.7	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
7.5.7	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
7.5.7	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
8.1.1	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
8.1.1	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。
8.1.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
8.1.1	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
8.1.1	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
8.1.1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
8.1.1	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
8.1.1	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
8.1.2	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
8.1.2	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
8.1.2	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
8.1.2	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) では、高可用性と耐障害性のために少なくとも 3 つのデータノードが必要です。少なくとも 3 つのデータノードを持つ OpenSearch Service ドメインをデプロイすると、ノードに障害が発生した場合のクラスターオペレーションが確実になります。
8.1.2	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	AWS 設定ルール	ガイダンス
8.1.3	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。
8.1.3	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	AWS 設定ルール	ガイダンス
8.1.3	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
8.1.3	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.1	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
8.4.1	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.1	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
8.4.1	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.1	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
8.4.1	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.1	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
8.4.1	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.1	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
8.4.1	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.1	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
8.4.2	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.2	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
8.4.2	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.2	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
8.4.2	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.2	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
8.4.2	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.2	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
8.4.2	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.2	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
8.4.2	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	AWS 設定ルール	ガイダンス
8.4.4	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
8.5.4	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	AWS 設定ルール	ガイダンス
8.5.4	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
9.1.1	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
9.1.1	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
9.1.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
9.1.1	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
9.1.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
9.1.1	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
9.1.1	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
9.1.1	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager シークレットのローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
9.1.1	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.1	secretsmanager-secret-periodic-rotation	このルールにより、 AWS Secrets Manager のシークレットで定期的なローテーションが有効になっていることが保証されます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。デフォルト値は 90 日です。
9.1.1	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
9.1.2	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.2	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.2	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
9.1.2	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.2	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
9.1.3	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
9.1.3	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.3	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
9.1.3	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.3	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
9.1.3	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
9.1.3	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.3	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
9.1.3	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.3	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
9.1.3	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.3	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
9.1.3	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.3	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.3	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.3	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
9.1.3	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.3	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.4	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.5	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
9.1.5	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.5	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
9.1.5	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.6	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.7	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.7	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
9.1.7	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.7	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.1.7	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
9.1.7	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.1	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
9.2.1	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
9.2.1	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.1	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
9.2.1	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
9.2.1	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.1	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.1	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.1	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.1	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
9.2.2	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
9.2.2	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.2	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
9.2.2	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.2	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
9.2.2	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.2	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
9.2.2	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.2	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.2.2	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
9.3.1	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
9.3.1	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
9.3.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
9.3.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
9.3.1	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
9.3.1	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
9.3.1	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
9.3.1	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
9.3.1	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
9.3.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
9.3.1	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
9.3.1	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
9.3.1	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
9.3.1	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
9.3.1	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
10.1.1	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
10.1.1	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.1.1	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
10.1.1	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
10.1.1	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
10.1.1	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.1.1	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
10.1.1	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
10.1.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
10.1.1	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
10.1.1	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
10.1.1	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
10.1.1	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.1.1	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.1.1	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
10.1.1	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
10.1.1	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
10.1.1	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.1.1	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
10.1.1	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
10.2.1	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
10.2.1	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
10.2.1	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
10.2.2	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
10.2.3	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。
10.2.3	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
10.2.3	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
11.1.1 (a)	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (a)	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
11.1.1 (a)	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.1 (a)	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (a)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
11.1.1 (a)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
11.1.1 (a)	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (a)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
11.1.1 (a)	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
11.1.1 (a)	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.1 (b)	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
11.1.1 (b)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
11.1.1 (b)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
11.1.1 (b)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
11.1.1 (b)	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.1 (b)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
11.1.1 (b)	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
11.1.1 (b)	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
11.1.1 (b)	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
11.1.1 (b)	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
11.1.1 (b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。
11.1.1 (b)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
11.1.1 (b)	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
11.1.1 (b)	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.1 (b)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.1 (b)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.1 (b)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
11.1.1 (b)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
11.1.1 (b)	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
11.1.1 (b)	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.1 (b)	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.1 (b)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.1 (b)	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.1 (b)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
11.1.1 (b)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.3	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
11.1.3	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
11.1.3	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
11.1.3	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.3	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
11.1.3	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
11.1.3	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
11.1.3	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
11.1.3	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
11.1.3	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
11.1.3	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。
11.1.3	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
11.1.3	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.3	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.3	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
11.1.3	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
11.1.3	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.3	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.1.3	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
11.1.3	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
11.2.1	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
11.2.2	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
11.2.2	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
11.2.2	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
11.2.2	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
11.2.2	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。
11.2.2	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
11.2.2	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
11.2.2	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
11.2.2	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
11.2.2	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
11.2.2	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.2	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。
11.2.4	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
11.2.4	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
11.2.4	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
11.2.4	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。
11.2.4	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
11.2.4	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
11.2.4	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
11.2.4	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
11.2.4	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
11.2.4	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	AWS 設定ルール	ガイダンス
11.2.4	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
11.2.4	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
11.3.1	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
11.3.5	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
11.3.5	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
11.3.5	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
11.3.5	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
11.4.2	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
11.4.2	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。
11.4.2	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
11.4.2	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
11.5.2	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
12.1.1	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
12.1.1	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
12.1.1	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
12.1.1	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
12.2.2	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
12.2.2	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.2	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
12.2.2	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
12.2.2	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.2	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
12.2.2	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
12.2.2	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.2	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
12.2.2	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.2	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.2	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.2	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
12.2.2	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.2	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
12.2.4	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.4	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
12.2.5	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.5	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.5	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
12.2.5	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
12.3.2	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
12.3.2	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	AWS 設定ルール	ガイダンス
12.3.2	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
14.1.2	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
14.1.2	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
14.1.2	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
14.1.2	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
14.1.2	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
14.1.2	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
14.1.2	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
14.1.2	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
14.1.2	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
14.1.3	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
14.1.3	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
14.1.3	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
14.1.3	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
14.2.2	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
14.2.2	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
14.2.2	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
14.2.2	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	AWS 設定ルール	ガイダンス
14.2.2	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
14.2.2	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
14.2.2	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
14.2.2	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
14.2.2	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
14.2.2	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
14.2.2	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
14.2.2	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
14.2.6	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	AWS 設定ルール	ガイダンス
14.2.6	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
14.2.6	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
14.2.6	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
14.2.6	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
14.2.6	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
14.2.6	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
14.2.6	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for MAS TRMG」で入手できます。

モニタリングの運用のベストプラクティス

このコンフォーマンスパックには、モニタリングに基づく AWS Config ルールが含まれています AWS。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Monitoring」で入手できます。

NBC の「TRMG」の運用のベストプラクティス

コンフォーマンスパックは、マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、カンボジア国立銀行 (NBC) の技術リスク管理 (TRM) ガイドラインフレームワークと AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の NBC TRM ガイドラインに関連付けられます。NBC の「TRM Guideline」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このサンプルコンフォーマンスパックテンプレートには、カンボジア国立銀行 (NBC) の技術リスク管理 (TRM) ガイドラインフレームワーク内のコントロールへのマッピングが含まれています。このフレームワークは、カンボジア国立銀行: 技術リスク管理ガイドラインからアクセスできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/または	iam-root-access-key-check	システムおよびアセットへのアクセスは、ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込む AWS アカウントのに役立つロールベ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	パスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とするユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		ースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベントの時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループが少なくとも 1 人のユーザーを持つようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (d)	d) 考慮すべき重要なコントロールには以下があります - - ユーザー ID とアクセスコントロールマトリックスの作成を適用し、承認する体系的なプロセス - リスク評価基くアクセス権限の付与 - 職務の効果的な分離を確保するために設計されたロールベースのアクセスコントロールの実装 - システムのデフォルトのユーザー名および/またはパスワードの変更、および汎用アカウントのユーザー ID とパスワードの共有の禁止 - ロールまたは責任の変更がある場合、アクセス権の採用/契約の停止に関するアクセス権の削除 - ユーザーの追加、削除、ロールの変更に関する情報セキュリティ機能をタイムリーに通知するプロセス - システム内のユーザー ID と実際にアクセスを必要とす	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	るユーザーとの定期的な照合、および不要な ID がある場合はその削除 - すべてのユーザーによる IT アセットへのアクセスの監査、記録、モニタリング - 重要なアプリケーションの長期休暇中のユーザーのユーザー ID の非アクティブ化の検討		
3.1.1(f)	f) 説明責任を果たすため、ユーザーと IT 資産が一意に特定され、その行動が監査可能であることを確認してください。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1(f)	f) 説明責任を果たすため、ユーザーと IT 資産が一意に特定され、その行動が監査可能であることを確認してください。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1(f)	f) 説明責任を果たすため、ユーザーと IT 資産が一意に特定され、その行動が監査可能であることを確認してください。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
3.1.1(f)	f) 説明責任を果たすため、ユーザーと IT 資産が一意に特定され、その行動が監査可能であることを確認してください。	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1(f)	f) 説明責任を果たすため、ユーザーと IT 資産が一意に特定され、その行動が監査可能であることを確認してください。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1(f)	f) 説明責任を果たすため、ユーザーと IT 資産が一意に特定され、その行動が監査可能であることを確認してください。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
3.1.1(f)	f) 説明責任を果たすため、ユーザーと IT 資産が一意に特定され、その行動が監査可能であることを確認してください。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。NIST SP 800-63 およびパスワード強度 AWS に関する Foundational Security Best Practices 標準に記載されている要件を満たしているか、それを超えています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基本的なセキュリティのベストプラクティス値： true)、 MinimumPasswordLength (AWS

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基盤セキュリティのベストプラクティス値： 90) IAM パスワードポリシー用。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「アクション」：「リソース」：「*」ではなく「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-root-access-key-check	システムおよびアセットへのアクセスは、ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込む AWS アカウントのに役立つロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムやアセットへのアクセスを制御するグループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベントの時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループが少なくとも 1 人のユーザーを持つようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1 (H)	h) 重要な業務を行うシステム管理者、セキュリティ担当者、プログラマーおよびスタッフは、職務機能と特権アクセスによって維持または運用する金融システムに重大な損害を与える能力を常に有します。システムへのアクセス権が昇格している担当者は、システム制御やセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステムのアクティビティを記録して綿密に監視する必要があります。以下に列挙するコントロールおよびセキュリティ対策のいくつかを考慮する必要があります。 - 特権ユーザーに対する二要素認証の実装 - 特権ユーザーによるリモートアクセスに対する強力なコントロールの導入 - 特権ユーザー数の制限 - 特	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	権ユーザーの「必要性」または「実行の必要性」に基づく特権的アクセス権の付与 - 特権ユーザーが実行するシステムアクティビティの監査ログの維持 - 特権ユーザーによる、自身のアクティビティがキャプチャされているシステムログへのアクセスの禁止 - ログの定期的な監査またはマネジメントレビューの実施 - 特権 ID およびアクセスコード - ベンダーおよび請負業者による、緊密な監督や監視のないシステムへの特権的アクセス権取得の禁止 - 不正アクセスからのバックアップデータの保護		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (a)	a) BFI は、ネットワーク境界を保護するために、ファイアウォール、ウイルス対策/マルウェア対策ソフトウェア、侵入検知および防止システムなどのネットワークセキュリティデバイスを IT インフラストラクチャの重要な分岐点にインストールする必要があります。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (a)	a) BFI は、ネットワーク境界を保護するために、ファイアウォール、ウイルス対策/マルウェア対策ソフトウェア、侵入検知および防止システムなどのネットワークセキュリティデバイスを IT インフラストラクチャの重要な分岐点にインストールする必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (a)	a) BFI は、ネットワーク境界を保護するために、ファイアウォール、ウイルス対策/マルウェア対策ソフトウェア、侵入検知および防止システムなどのネットワークセキュリティデバイスを IT インフラストラクチャの重要な分岐点にインストールする必要があります。	api-gw-associated-with-waf	AWS WAF を使用すると、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれます) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基盤セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	[api-gw-execution-logging-enabled](#)	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベントの時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	ebs-snapshot-public-restorable-check	EBS スナップショットがパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private Cloud (Amazon VPC) 内にあることを確認 AWS して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	emr-master-no-public-ip	Amazon EMR クラスターマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの入出力ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、入出力ネットワークトラフィックを AWS リソースにステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (c)	c) ネットワーク内の情報のセキュリティを確保し、不正なアクセスから接続されたサービスを保護するためのコントロールを実装する必要があります。特に、以下の項目を考慮する必要があります。 - ネットワーク機器の管理に関する責任と手順を確立する。 - ネットワークの運用責任をコンピュータの運用から適切に分離する。 - パブリックネットワークまたはワイヤレスネットワークを通過するデータの機密性と完全性を保護し、接続されたシステムやアプリケーションを保護するための特別なコントロールを確立する (信頼できないシステムやネットワークに接続する場合、ネットワーク暗号化プロトコルを含む) - 情報セキュリティに影響を与える、または関連するアクショ	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントは、SSM ドキュメントへの意図しないアクセスを許可する可能性があるため、公開されていないことを確認してください。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ンの記録と検出を可能にするために、適切なログ記録とモニタリングを適用する必要がある。 - 管理活動は、組織へのサービスを最適化するため、また、情報処理インフラストラクチャ全体に一貫したコントロールを適用するために、緊密に連携する必要がある。 - ネットワーク上のシステムには認証を必要とし - 信頼できないシステムによるネットワークへの接続には制限を必要とする。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基盤セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2 (e)	e) ネットワークサービスは、シンプルで管理の不要な帯域幅から、VPN、Voice over IP、VSAT などの高度なサービスまで、多岐にわたります。ネットワークサービスのセキュリティ機能は、以下のようなものである必要があります。 - 認証、暗号化、ネットワーク接続制御などのネットワークサービスのセキュリティに適用されるテクノロジー - セキュリティおよびネットワーク接続のルールに従った、ネットワークサービスとのセキュアな接続に必要なテクノロジーによるパラメータ - ネットワークサービスまたはアプリケーションへのアクセスを制限するためのネットワークサービスの使用手順 (必要な場合)	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基盤セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (e)	e) 暗号化を使用して、リモートアクセスデバイスと施設間の通信チャネルを保護し、ネットワークのなりすましに関連するリスクを制限します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベントの時刻が含まれます。
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
3.1.3 (g)	g) リモートアクセス通信のログを保持します。ログには、リモートアクセスを通じて実行されるすべてのアクティビティを含む、すべてのリモートアクセスの日付、時間、ユーザー、ユーザーの場所、期間、および目的が含まれている必要があります。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (i)	i) リモートアクセスのための二要素認証プロセス (例: ワンタイムランダムパスワード生成を備えた PIN ベースのトークンカードまたはトークンベースの PKI) を徹底します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (i)	i) リモートアクセスのための二要素認証プロセス (例: ワンタイムランダムパスワード生成を備えた PIN ベースのトークンカードまたはトークンベースの PKI) を徹底します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (i)	i) リモートアクセスのための二要素認証プロセス (例: ワンタイムランダムパスワード生成を備えた PIN ベースのトークンカードまたはトークンベースの PKI) を徹底します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3 (i)	i) リモートアクセスのための二要素認証プロセス (例: ワンタイムランダムパスワード生成を備えた PIN ベースのトークンカードまたはトークンベースの PKI) を徹底します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4 (c)(e)	c) パッチ管理プロセスには、以下の側面を含める必要があります。 - パッチが許可されたソースからのものであることを確認するためのパッチの取得と検証の方法の決定 - 組織で使用されるアプリケーションやシステムに適用可能な脆弱性の特定方法 - パッチを実装する (または特定のパッチを実装しない) ことによるビジネスへの影響の評価 - パッチがテストされていることの確認 - パッチのデプロイ方法の説明 (例: 自動的) - 組織全体でのパッチデプロイの状況に関するレポート - パッチデプロイの失敗への対処方法 (例: パッチの再デプロイ) を含める e) BFI は、自動化されたパッチ管理ツールとソフトウェア更新ツールを、それらのツールを利用できるすべての安全なシステム	ec2-instance-managed-by-systems-manager	Systems AWS Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	にデプロイする必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4 (c)(e)	c) パッチ管理プロセスには、以下の側面を含める必要があります。 - パッチが許可されたソースからのものであることを確認するためのパッチの取得と検証の方法の決定 - 組織で使用されるアプリケーションやシステムに適用可能な脆弱性の特定方法 - パッチを実装する (または特定のパッチを実装しない) ことによるビジネスへの影響の評価 - パッチがテストされていることの確認 - パッチのデプロイ方法の説明 (例: 自動的) - 組織全体でのパッチデプロイの状況に関するレポート - パッチデプロイの失敗への対処方法 (例: パッチの再デプロイ) を含める e) BFI は、自動化されたパッチ管理ツールとソフトウェア更新ツールを、それらのツールを利用できるすべての安全なシステム	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations を使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを支援します。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	にデプロイする必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4 (c)(e)	c) パッチ管理プロセスには、以下の側面を含める必要があります。 - パッチが許可されたソースからのものであることを確認するためのパッチの取得と検証の方法の決定 - 組織で使用されるアプリケーションやシステムに適用可能な脆弱性の特定方法 - パッチを実装する (または特定のパッチを実装しない) ことによるビジネスへの影響の評価 - パッチがテストされていることの確認 - パッチのデプロイ方法の説明 (例: 自動的) - 組織全体でのパッチデプロイの状況に関するレポート - パッチデプロイの失敗への対処方法 (例: パッチの再デプロイ) を含める e) BFI は、自動化されたパッチ管理ツールとソフトウェア更新ツールを、それらのツールを利用できるすべての安全なシステム	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている AWS Systems Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	にデプロイする必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4 (c)(e)	c) パッチ管理プロセスには、以下の側面を含める必要があります。 - パッチが許可されたソースからのものであることを確認するためのパッチの取得と検証の方法の決定 - 組織で使用されるアプリケーションやシステムに適用可能な脆弱性の特定方法 - パッチを実装する (または特定のパッチを実装しない) ことによるビジネスへの影響の評価 - パッチがテストされていることの確認 - パッチのデプロイ方法の説明 (例: 自動的) - 組織全体でのパッチデプロイの状況に関するレポート - パッチデプロイの失敗への対処方法 (例: パッチの再デプロイ) を含める e) BFI は、自動化されたパッチ管理ツールとソフトウェア更新ツールを、それらのツールを利用できるすべての安全なシステム	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	にデプロイする必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4 (c)(e)	c) パッチ管理プロセスには、以下の側面を含める必要があります。 - パッチが許可されたソースからのものであることを確認するためのパッチの取得と検証の方法の決定 - 組織で使用されるアプリケーションやシステムに適用可能な脆弱性の特定方法 - パッチを実装する (または特定のパッチを実装しない) ことによるビジネスへの影響の評価 - パッチがテストされていることの確認 - パッチのデプロイ方法の説明 (例: 自動的) - 組織全体でのパッチデプロイの状況に関するレポート - パッチデプロイの失敗への対処方法 (例: パッチの再デプロイ) を含める e) BFI は、自動化されたパッチ管理ツールとソフトウェア更新ツールを、それらのツールを利用できるすべての安全なシステム	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	にデプロイする必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4 (c)(e)	c) パッチ管理プロセスには、以下の側面を含める必要があります。 - パッチが許可されたソースからのものであることを確認するためのパッチの取得と検証の方法の決定 - 組織で使用されるアプリケーションやシステムに適用可能な脆弱性の特定方法 - パッチを実装する (または特定のパッチを実装しない) ことによるビジネスへの影響の評価 - パッチがテストされていることの確認 - パッチのデプロイ方法の説明 (例: 自動的) - 組織全体でのパッチデプロイの状況に関するレポート - パッチデプロイの失敗への対処方法 (例: パッチの再デプロイ) を含める e) BFI は、自動化されたパッチ管理ツールとソフトウェア更新ツールを、それらのツールを利用できるすべての安全なシステム	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	にデプロイする必要があります。		
3.1.5 (d)(e)	d) 適切なキー管理には、暗号化キーの生成、保存、アーカイブ、取得、配布、廃棄、破棄のための安全なプロセスが必要です。e) すべての暗号化キーを、変更や紛失から保護する必要があります。また、シークレットキーやプライベートキーは、不正使用や漏洩から保護する必要があります。キーの生成、保存、保管に使用する機器には、物理的な保護が必要です。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (d)(e)	d) 適切なキー管理には、暗号化キーの生成、保存、アーカイブ、取得、配布、廃棄、破棄のための安全なプロセスが必要です。e) すべての暗号化キーを、変更や紛失から保護する必要があります。また、シークレットキーやプライベートキーは、不正使用や漏洩から保護する必要があります。キーの生成、保存、保管に使用する機器には、物理的な保護が必要です。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (d)(e)	d) 適切なキー管理には、暗号化キーの生成、保存、アーカイブ、取得、配布、廃棄、破棄のための安全なプロセスが必要です。e) すべての暗号化キーを、変更や紛失から保護する必要があります。また、シークレットキーやプライベートキーは、不正使用や漏洩から保護する必要があります。キーの生成、保存、保管に使用する機器には、物理的な保護が必要です。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (d)(e)	d) 適切なキー管理には、暗号化キーの生成、保存、アーカイブ、取得、配布、廃棄、破棄のための安全なプロセスが必要です。e) すべての暗号化キーを、変更や紛失から保護する必要があります。また、シークレットキーやプライベートキーは、不正使用や漏洩から保護する必要があります。キーの生成、保存、保管に使用する機器には、物理的な保護が必要です。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (f)	f) キー管理システムは、以下の合意済みの一連の標準、手順、および安全な方法に基づいている必要があります。 - さまざまな暗号システムおよびさまざまなアプリケーションのキーを生成する - パブリックキーの証明書を発行および取得する - 目的のエンティティへのキーと、キーを受け取った際の有効化の方法の配布 - キーの保存と、権限のあるユーザーによるキーへのアクセス方法 - キーの変更または更新およびキーの変更時期とその方法に関するルール - 侵害されたキーの処理 - キーが侵害された場合や、ユーザーが組織を離れた場合などのキーの回収方法をなど、キーの取り消しまたは非アクティブ化 (キーをアーカイブする必要もある場合) - 紛失または破損したキーの	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	復旧 - キーのバックアップまたはアーカイブ - キーの破棄 - キー管理に関連するアクティビティのログ記録と監査。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (f)	f) キー管理システムは、以下の合意済みの一連の標準、手順、および安全な方法に基づいている必要があります。 - さまざまな暗号システムおよびさまざまなアプリケーションのキーを生成する - パブリックキーの証明書を発行および取得する - 目的のエンティティへのキーと、キーを受け取った際の有効化の方法の配布 - キーの保存と、権限のあるユーザーによるキーへのアクセス方法 - キーの変更または更新およびキーの変更時期とその方法に関するルール - 侵害されたキーの処理 - キーが侵害された場合や、ユーザーが組織を離れた場合などのキーの回収方法をなど、キーの取り消しまたは非アクティブ化 (キーをアーカイブする必要もある場合) - 紛失または破損したキーの	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	復旧 - キーのバックアップまたはアーカイブ - キーの破棄 - キー管理に関連するアクティビティのログ記録と監査。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (f)	f) キー管理システムは、以下の合意済みの一連の標準、手順、および安全な方法に基づいている必要があります。 - さまざまな暗号システムおよびさまざまなアプリケーションのキーを生成する - パブリックキーの証明書を発行および取得する - 目的のエンティティへのキーと、キーを受け取った際の有効化の方法の配布 - キーの保存と、権限のあるユーザーによるキーへのアクセス方法 - キーの変更または更新およびキーの変更時期とその方法に関するルール - 侵害されたキーの処理 - キーが侵害された場合や、ユーザーが組織を離れた場合などのキーの回収方法をなど、キーの取り消しまたは非アクティブ化 (キーをアーカイブする必要もある場合) - 紛失または破損したキーの	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基盤セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	復旧 - キーのバックアップまたはアーカイブ - キーの破棄 - キー管理に関連するアクティビティのログ記録と監査。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (f)	f) キー管理システムは、以下の合意済みの一連の標準、手順、および安全な方法に基づいている必要があります。 - さまざまな暗号システムおよびさまざまなアプリケーションのキーを生成する - パブリックキーの証明書を発行および取得する - 目的のエンティティへのキーと、キーを受け取った際の有効化の方法の配布 - キーの保存と、権限のあるユーザーによるキーへのアクセス方法 - キーの変更または更新およびキーの変更時期とその方法に関するルール - 侵害されたキーの処理 - キーが侵害された場合や、ユーザーが組織を離れた場合などのキーの回収方法をなど、キーの取り消しまたは非アクティブ化 (キーをアーカイブする必要もある場合) - 紛失または破損したキーの	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	復旧 - キーのバックアップまたはアーカイブ - キーの破棄 - キー管理に関連するアクティビティのログ記録と監査。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (f)	f) キー管理システムは、以下の合意済みの一連の標準、手順、および安全な方法に基づいている必要があります。 - さまざまな暗号システムおよびさまざまなアプリケーションのキーを生成する - パブリックキーの証明書を発行および取得する - 目的のエンティティへのキーと、キーを受け取った際の有効化の方法の配布 - キーの保存と、権限のあるユーザーによるキーへのアクセス方法 - キーの変更または更新およびキーの変更時期とその方法に関するルール - 侵害されたキーの処理 - キーが侵害された場合や、ユーザーが組織を離れた場合などのキーの回収方法をなど、キーの取り消しまたは非アクティブ化 (キーをアーカイブする必要もある場合) - 紛失または破損したキーの	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	復旧 - キーのバックアップまたはアーカイブ - キーの破棄 - キー管理に関連するアクティビティのログ記録と監査。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (f)	f) キー管理システムは、以下の合意済みの一連の標準、手順、および安全な方法に基づいている必要があります。 - さまざまな暗号システムおよびさまざまなアプリケーションのキーを生成する - パブリックキーの証明書を発行および取得する - 目的のエンティティへのキーと、キーを受け取った際の有効化の方法の配布 - キーの保存と、権限のあるユーザーによるキーへのアクセス方法 - キーの変更または更新およびキーの変更時期とその方法に関するルール - 侵害されたキーの処理 - キーが侵害された場合や、ユーザーが組織を離れた場合などのキーの回収方法をなど、キーの取り消しまたは非アクティブ化 (キーをアーカイブする必要もある場合) - 紛失または破損したキーの	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	復旧 - キーのバックアップまたはアーカイブ - キーの破棄 - キー管理に関連するアクティビティのログ記録と監査。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5 (f)	f) キー管理システムは、以下の合意済みの一連の標準、手順、および安全な方法に基づいている必要があります。 - さまざまな暗号システムおよびさまざまなアプリケーションのキーを生成する - パブリックキーの証明書を発行および取得する - 目的のエンティティへのキーと、キーを受け取った際の有効化の方法の配布 - キーの保存と、権限のあるユーザーによるキーへのアクセス方法 - キーの変更または更新およびキーの変更時期とその方法に関するルール - 侵害されたキーの処理 - キーが侵害された場合や、ユーザーが組織を離れた場合などのキーの回収方法をなど、キーの取り消しまたは非アクティブ化 (キーをアーカイブする必要もある場合) - 紛失または破損したキーの	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	復旧 - キーのバックアップまたはアーカイブ - キーの破棄 - キー管理に関連するアクティビティのログ記録と監査。		
3.1.6 (a)	a) BFI は、自動化されたツールと手動による手法を組み合わせてデプロイし、包括的な VA を定期的に実行する必要があります。ウェブベースの外部向けシステムの場合、VA の範囲には、SQL インジェクションやクロスサイトスクリプティングなどの一般的なウェブの脆弱性を含める必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.6 (a)	a) BFI は、自動化されたツールと手動による手法を組み合わせてデプロイし、包括的な VA を定期的に実行する必要があります。ウェブベースの外部向けシステムの場合、VA の範囲には、SQL インジェクションやクロスサイトスクリプティングなどの一般的なウェブの脆弱性を含める必要があります。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.6 (a)	a) BFI は、自動化されたツールと手動による手法を組み合わせてデプロイし、包括的な VA を定期的に実行する必要があります。ウェブベースの外部向けシステムの場合、VA の範囲には、SQL インジェクションやクロスサイトスクリプティングなどの一般的なウェブの脆弱性を含める必要があります。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれます) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
3.1.6(c)	c) BFI は、VA & PT で特定された問題を是正するプロセスを確立し、その後に是正措置の再検証を実施して、ギャップが完全に対処されていることを確認すべきである。	vuln-mitigated-accepted (Process Check)	新たに特定された脆弱性が修正されるか、受け入れられたリスクとしてドキュメント化されるようにします。組織のコンプライアンス要件に従って、脆弱性を修正するか、リスクとして承諾する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.6 (f)	f) セキュリティ機能は、軽減されない各部門の重大な脆弱性の数に関するステータスの更新と軽減のための計画を、定期的に上級管理職に提供します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.8	User training and awareness	security-awareness-program-exists(Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するために、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するために、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	redshift-cluster-kms-enabled	保管中のデータを保護するために、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.10 (b)	b) システムドキュメント、アプリケーションのソースコード、本番トランザクションデータなどの機密情報には、改ざんを防止するためのより広範なコントロールが必要です (例: 完全性チェッカー、暗号学的ハッシュ)。さらに、ポリシーによって、情報が含まれる印刷物などの機密情報の配布を最小限に抑える必要があります。	secretsmanager-using-cmk	保管中のデータを保護するために、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	dynamodb-in-backup-plan	データバックアッププロセスを支援するには、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	ebs-in-backup-plan	データバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	efs-in-backup-plan	データバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	rds-in-backup-plan	データバックアッププロセスを支援するには、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (h)	h) 変更にともなうリスクを最小限に抑えるため、BFI は、影響を受けるシステムやアプリケーションのバックアップを変更前に実行する必要があります。BFI は、デプロイ中またはデプロイ後に問題が発生した場合に、システムまたはアプリケーションを以前のバージョンに戻すためのロールバックの計画を確立する必要があります。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベントの時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
3.2.1 (k)	k) 監査ログやセキュリティログは、調査やトラブルシューティングを容易にする有用な情報です。BFIは、移行プロセス中に実行されたアクティビティを記録するため、ログ機能が有効になっていることを確認する必要があります。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.3 (a)	a) 情報セキュリティインシデントを防止、検出、分析し、対応するためのプロセスを開発し、実装します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.3 (a)	a) 情報セキュリティインシデントを防止、検出、分析し、対応するためのプロセスを開発し、実装します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自動スケーリングは、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
3.3.1 (a)	a) システム設計の一環として、システムの高可用性、適切な容量、信頼性の高いパフォーマンス、高速な応答時間、スケーラビリティの維持に関連する重要な要素を考慮します。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベントの時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (a)(b)(c)(f)(j)	a) 監査とレビューの目的で、ユーザのアクセス記録が一意に識別され、記録されていることを確認します。b) 不正アクセスの説明責任と識別についてドキュメント化されていることを確認します。c) 特権ユーザによって実行される、システムでのアクティビティの監査ログを有効にします。f) 情報セキュリティに影響を与える可能性のある、または関連するアクティビティの記録と検出を行うため、適切なログ記録とモニタリングが適用されることを確認します。j) イベントのログ記録によって、システムのセキュリティに関する統合レポートとアラートを生成できる自動モニタリングシステムの土台が設定されることを確認します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4(f)	f) 情報セキュリティに影響を及ぼす可能性がある、または情報セキュリティに関連する行動を記録および検出できるように、適切なログ記録とモニタリングを適用する必要があります。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベントの時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4 (g)	g) 関連する場合、イベントログに以下が含まれていることを確認します。 - ユーザー ID - システムのアクティビティ - ログオンおよびログオフなど主要なイベントの日時と詳細 - 可能な場合、デバイスの ID またはロケーションおよびシステム識別子 - システムにおけるアクセス試行の成功と拒否の記録 - データやその他のリソースへのアクセス試行の成功と拒否の記録 - システム設定の変更 - 特権の使用 - システムユーティリティとアプリケーションの使用 - アクセスされたファイルとアクセスの種類 - ネットワークアドレスとプロトコル - アクセスコントロールシステムにより発生したアラーム - アプリケーションおよびオンラインの顧客トランザクションでユーザーが実行	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	したトランザクションの記録		
3.6.1 (a)(h)	a) BFI は、ウェブアプリケーションに適切なセキュリティ対策を講じ、さまざまなウェブ上のセキュリティリスクに対して合理的な緩和策を講じる必要があります。h) BFI は、ウェブアプリケーションに適切なセキュリティ対策を講じ、さまざまなウェブ上のセキュリティリスクに対して合理的な緩和策を講じる必要があります。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (a)(h)	a) BFI は、ウェブアプリケーションに適切なセキュリティ対策を講じ、さまざまなウェブ上のセキュリティリスクに対して合理的な緩和策を講じる必要があります。h) BFI は、ウェブアプリケーションに適切なセキュリティ対策を講じ、さまざまなウェブ上のセキュリティリスクに対して合理的な緩和策を講じる必要があります。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれます) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基盤セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (b)	b) BFI は、インターネットバンキングシステムやその他の関連システムに関連するセキュリティ要件を評価し、要求される機密性と完全性の度合いを考慮した暗号化ソリューションを採用する必要があります。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスと内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (d)	d) b) インターネットバンキングを提供する BFI は、DDoS 攻撃の兆候を示している可能性のある、ネットワークの異常なトラフィック状況やシステムパフォーマンス、システムリソースの使用量の急増に対応する必要があります。したがって、事前と事後の対策が成功するかどうかは、ネットワークやシステムの異常を効果的に検知、モニタリング、分析するための適切なツールのデプロイに左右されます。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (d)	d) b) インターネットバンキングを提供する BFI は、DDoS 攻撃の兆候を示している可能性のある、ネットワークの異常なトラフィック状況やシステムパフォーマンス、システムリソースの使用量の急増に対応する必要があります。したがって、事前と事後の対策が成功するかどうかは、ネットワークやシステムの異常を効果的に検知、モニタリング、分析するための適切なツールのデプロイに左右されます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (d)	d) b) インターネットバンキングを提供する BFI は、DDoS 攻撃の兆候を示している可能性のある、ネットワークの異常なトラフィック状況やシステムパフォーマンス、システムリソースの使用量の急増に対応する必要があります。したがって、事前と事後の対策が成功するかどうかは、ネットワークやシステムの異常を効果的に検知、モニタリング、分析するための適切なツールのデプロイに左右されます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (d)	d) b) インターネットバンキングを提供する BFI は、DDoS 攻撃の兆候を示している可能性のある、ネットワークの異常なトラフィック状況やシステムパフォーマンス、システムリソースの使用量の急増に対応する必要があります。したがって、事前と事後の対策が成功するかどうかは、ネットワークやシステムの異常を効果的に検知、モニタリング、分析するための適切なツールのデプロイに左右されます。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (d)	d) b) インターネットバンキングを提供する BFI は、DDoS 攻撃の兆候を示している可能性のある、ネットワークの異常なトラフィック状況やシステムパフォーマンス、システムリソースの使用量の急増に対応する必要があります。したがって、事前と事後の対策が成功するかどうかは、ネットワークやシステムの異常を効果的に検知、モニタリング、分析するための適切なツールのデプロイに左右されます。	[api-gw-associated-with-waf](#)	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれます) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1 (e)	e) BFI は、情報セキュリティの脆弱性を定期的に評価し、IT セキュリティの既存のリスクマネジメントフレームワークの有効性を評価し、新たな脆弱性にタイムリーに対処するために必要な調整を行う必要があります。この評価は、重要な変更の一部としても実施する必要があります。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	ebs-snapshot-public-restorable-check	EBS スナップショットがパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private Cloud (Amazon VPC) 内にあることを確認 AWS して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	emr-master-no-public-ip	Amazon EMR クラスターマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、入出力ネットワークトラフィックを AWS リソースにステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの入出力ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4 (a)(b)	a) インターネットアクセスを制限し、重要なシステムを一般的な IT 環境から分離します。b) 攻撃の対象となる領域を削減し、脆弱性を軽減します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NBC TRMG」で入手できます。

NERC CIP BCSI に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、BES サイバーシステム情報 (BCSI) に関する北米電力信頼性公社 の「Critical Infrastructure Protection Standards (NERC CIP)」、CIP-004-7」、CIP-011-3」、および AWS Config マネージドルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、BCSI に適用される 1 つ以上の NERC CIP コントロールに関連付けられます。NERC の「CIP」

によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へ	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールは、Amazon OpenSearch ドメインへの最小特権アクセスを実現するための強化された承認メカニズムを提供します。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、OpenSearch ダッシュボードのマルチテナンシーのサポート、OpenSearch と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	のアクセス手段 (例: 物理的なキーまたはアクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へのアクセス手段 (例: 物理的なキーまたは	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	アクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へのアクセス手段 (例: 物理的なキーまたは	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	アクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へのアクセス手段 (例: 物理的なキーまたは	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	アクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へのアクセス手段 (例: 物理的なキーまたは	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	アクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へのアクセス手段 (例: 物理的なキーまたは	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	アクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へのアクセス手段 (例: 物理的なキーまたは	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	アクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へのアクセス手段 (例: 物理的なキーまたは	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	アクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へのアクセス手段 (例: 物理的なキーまたは	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	アクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-004-7-R6-Part 6.1	各責任主体は、CIP-004-7 Table R6 - Access Management Program for BES Cyber System Information の該当する各要件部分のまとめを含む、CIP-004-7 Table R6 - Access Management for BES Cyber System Information で特定される「対象システム」に関連する BCSI へのプロビジョニングされたアクセスを承認、検証、および取り消すため、1 つ以上のドキュメント化されたアクセスマネジメントプログラムを実装するものとします。この要件のコンテキストで BCSI へのアクセスと見なされるために、個人は BCSI を入手する機能と利用する機能の両方を持っている必要があります。プロビジョニングされたアクセスは、BCSI へのアクセス手段 (例: 物理的なキーまたは	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	アクセスカード、ユーザーおよび関連する権利と特権、暗号化キー) を個人に提供するために実行される特定のアクションの結果と見なされます。Part 6.1: プロビジョニングの前に、CIP Exceptional Circumstances: 6.1.1 を除き、責任主体の決定に従い、必要性に基づいて承認 (Part 4.1 に従って既に承認されている場合を除く) します。電子的な BCSI へのプロビジョニングされた電子アクセス		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	ecr-private-tag-immutability-enabled	Elastic Container Repository (ECR) のタグ不変性を有効にして、ECR イメージのイメージタグが上書きされないようにします。以前は、タグが上書きされる可能性があり、手作業でイメージを一意に識別するための手法が必要でした。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、Amazon OpenSearch と Amazon VPC 内の他のサービスの間で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	s3-event-notifications-enabled	Amazon S3 イベント通知により、バケットオブジェクトに対する偶発的または意図的な変更について、関連する担当者に警告できます。アラートの例としては、新しいオブジェクトの作成、オブジェクトの削除、オブジェクトの復元、オブジェクトの紛失およびレプリケートなどが含まれます。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	s3-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	rds-cluster-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Relational Database Service (Amazon RDS) データベースクラスターのアタックサーフェスを減らすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	rds-instance-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Relational Database Service (Amazon RDS) データベースインスタンスのアタックサーフェスを減らすことができます。
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	redshift-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Redshift クラスターのアタックサーフェスを減らすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CIP-011-3-R1-Part 1.2	各責任主体は、CIP-011-3 Table R1 – Information Protection に記載された該当する各要件部分のまとめを含む、1 つ以上のドキュメント化された情報保護プログラムを実装するものとします。Part 1.2: 機密性を侵害するリスクを軽減するために、BCSI を保護し、安全に処理する方法。	s3-bucket-acl-prohibited	このルールは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NERC CIP BCSI」で入手できます。

NCSC Cloud Security Principles に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するよう

には設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、英国国家サイバーセキュリティセンター (NCSC) のクラウドセキュリティ原則と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の UK NCSC Cloud Security Principles コントロールに関連付けられます。英国の NCSC の「Cloud Security Principles」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックのサンプルテンプレートには、英国の NCSC の「Cloud Security Principles (National Cyber Security Center | Cloud security guidance)」内のコントロールへのマッピングが含まれており、それらの公共部門に関する情報は Open Government License v3.0 のライセンスを取得しています。Open Government Licence には、こちらからアクセスできます。「公共部門の情報のための Open Government Licence」

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴か	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすること

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ら適切に保護する必要があります。		で、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
1. 転送中のデータの保護	ネットワークを通過するユーザーデータは、改ざんや盗聴から適切に保護する必要があります。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトに対して暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2. アセットの保護と回復性	お客様のデータ (およびそれを保存または処理するアセット) は適切に保護する必要があります。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5. 運用上のセキュリティ	サービスは、攻撃を妨げ、検出し、または防止する方法で運用および管理する必要があります。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7. 安全な開発	クラウドサービスは、セキュリティへの脅威を最小限に抑え、軽減する方法で設計、開発、デプロイする必要があります。	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。
7. 安全な開発	クラウドサービスは、セキュリティへの脅威を最小限に抑え、軽減する方法で設計、開発、デプロイする必要があります。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7. 安全な開発	クラウドサービスは、セキュリティへの脅威を最小限に抑え、軽減する方法で設計、開発、デプロイする必要があります。	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
9. 安全なユーザー管理	プロバイダーは、サービスの使用を安全に管理するためのツールを用意する必要があります。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	rds-instance-iam-authentication-enabled	システムおよびアセットへのアクセスを制御するために、Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。これにより、データベースに出入りするネットワークトラフィックが、Secure Sockets Layer (SSL) を使用して暗号化されるようになります。認証は外部で管理されるため、ユーザー認証情報をデータベースに保存する必要はありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10. ID と認証	サービスインターフェイスへのアクセスは、認証された権限のある個人に限定する必要があります。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	ecs-container-insights-enabled	モニタリングは、Amazon Elastic Container Service (ECS) と AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。Container Insights では、問題の迅速な特定と解決に役立つ、コンテナの再起動失敗などの診断情報も提供されます。
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11. 外部インターフェイスの保護	サービスへの外部インターフェイスまたは信頼性の低いインターフェイスをすべて特定して保護する必要があります。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12. Secure service administration	クラウドプロバイダーは、管理システムの価値が高いことを認識する必要があります。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13. ユーザーの監査情報	プロバイダーは、サービスへのアクセスを監視するために必要なログと、サービス内に保持されているデータを提供する必要があります。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
13. ユーザーの監査情報	プロバイダーは、サービスへのアクセスを監視するために必要なログと、サービス内に保持されているデータを提供する必要があります。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13. ユーザーの監査情報	プロバイダーは、サービスへのアクセスを監視するために必要なログと、サービス内に保持されているデータを提供する必要があります。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
13. ユーザーの監査情報	プロバイダーは、サービスへのアクセスを監視するために必要なログと、サービス内に保持されているデータを提供する必要があります。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NCSC Cloud Security Principles」で入手できます。

NCSC の「Cyber Assesment Framework」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、英国国家サイバーセキュリティセンター (NCSC) の「Cyber Assessment Framework (CAF)」によるコントロールと Config AWS マネージドルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の UK NCSC CAF コントロールに関連付けられます。英国のNCSC の「CAF」によるコントロールを、複数の Config ルールに関連付ける

ことができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックのサンプルテンプレートには、英国のNCSC の「CAF (National Cyber Security Centre | NCSC CAF)」内のガイダンスへのマッピングが含まれており、それらの公共部門に関する情報は Open Government License v3.0 のライセンスを取得しています。Open Government Licence には、こちらからアクセスできます。「公共部門の情報のための Open Government Licence」

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.a#アセットマネジメント	重要な機能の運用に必要なネットワークや情報システムの提供、維持、サポートに必要なすべてが決定され、理解されている。これにはデータ、人、システム、それを支えるインフラストラクチャ (電力や冷却など) が含まれます。	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。
A3.a#アセットマネジメント	重要な機能の運用に必要なネットワークや情報システムの提供、維持、サポートに必要なすべてが決定され、理解されている。これにはデータ、人、システム、それを支えるインフ	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのイン

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ラストラクチャ (電力や冷却など) が含まれます。		ベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
A3.a#アセットマネジメント	重要な機能の運用に必要なネットワークや情報システムの提供、維持、サポートに必要なすべてが決定され、理解されている。これにはデータ、人、システム、それを支えるインフラストラクチャ (電力や冷却など) が含まれます。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.a#アセットマネジメント	重要な機能の運用に必要なネットワークや情報システムの提供、維持、サポートに必要なすべてが決定され、理解されている。これにはデータ、人、システム、それを支えるインフラストラクチャ (電力や冷却など) が含まれます。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.a#アセットマネジメント	重要な機能の運用に必要なネットワークや情報システムの提供、維持、サポートに必要なすべてが決定され、理解されている。これにはデータ、人、システム、それを支えるインフラストラクチャ (電力や冷却など) が含まれます。	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a#Identity Verification, Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.a Identity Verification,Authentication and Authorisation	重要な機能をサポートするネットワークや情報システムへのアクセスを強固に検証し、認証し、権限を与えます。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.b Device Management	本質的な機能を支えるネットワーク、情報システム、データにアクセスするために使用されるデバイスを十分に理解し、信頼できます。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.b Device Management	本質的な機能を支えるネットワーク、情報システム、データにアクセスするために使用されるデバイスを十分に理解し、信頼できます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.c Privileged User Management	必須機能をサポートするネットワークや、情報システムへの特権的なユーザーアクセスを綿密に管理することができます。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d#Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B2.d Identity and Access Management (IdAM)	必須機能をサポートするネットワークや情報システムにおいて、ID やアクセス制御の適切な管理や保守を保証します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.a Understanding Data	必須機能のオペレーションに重要なデータ、その保存場所、移動先、利用不能または不正アクセス、修正、削除が必須機能にどのような悪影響を及ぼすかを十分に理解していること。#これは本質的な機能の運用に重要なデータを保存またはアクセスするサードパーティーについても適用されます。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.b Data in Transit	本質的な機能の運用に重要なデータの転送を保護しました。これには、サードパーティーへのデータ転送が含まれます。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
B3.c Stored Data	必須機能のオペレーションに重要な保存データを保護しました。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.a Secure by Design	必須機能の運用を支えるネットワークや情報システムにセキュリティを設計します。攻撃対象領域を最小化し、単一の脆弱性が悪用されることによって基本機能の運用が影響を受けることがないようにします。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.b Secure Configuration	重要な機能の運用を支えるネットワークと情報システムを安全に設定することができます。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.b Secure Configuration	重要な機能の運用を支えるネットワークと情報システムを安全に設定することができます。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.b Secure Configuration	重要な機能の運用を支えるネットワークと情報システムを安全に設定することができます。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.b Secure Configuration	重要な機能の運用を支えるネットワークと情報システムを安全に設定することができます。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.c# Secure Management	セキュリティの確保と維持を可能にするために、必須機能の運用をサポートする組織のネットワークと情報システムを管理します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.c# Secure Management	セキュリティの確保と維持を可能にするために、必須機能の運用をサポートする組織のネットワークと情報システムを管理します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.c# Secure Management	セキュリティの確保と維持を可能にするために、必須機能の運用をサポートする組織のネットワークと情報システムを管理します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.d。Vulnerability Management	ネットワークや情報システムの既知の脆弱性を管理し、必須機能に悪影響が及ばないようにする。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.d。Vulnerability Management	ネットワークや情報システムの既知の脆弱性を管理し、必須機能に悪影響が及ばないようにする。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.d。Vulnerability Management	ネットワークや情報システムの既知の脆弱性を管理し、必須機能に悪影響が及ばないようにする。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.d。Vulnerability Management	ネットワークや情報システムの既知の脆弱性を管理し、必須機能に悪影響が及ばないようにする。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.d。Vulnerability Management	ネットワークや情報システムの既知の脆弱性を管理し、必須機能に悪影響が及ばないようにする。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B4.d。Vulnerability Management	ネットワークや情報システムの既知の脆弱性を管理し、必須機能に悪影響が及ばないようにする。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.b Design for Resilience	サイバーセキュリティのインシデントに耐えられるように、重要な機能を支えるネットワークと情報システムを設計します。システムは適切に分離され、リソースの制限は緩和されます。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.b Design for Resilience	サイバーセキュリティのインシデントに耐えられるように、重要な機能を支えるネットワークと情報システムを設計します。システムは適切に分離され、リソースの制限は緩和されます。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
B5.b Design for Resilience	サイバーセキュリティのインシデントに耐えられるように、重要な機能を支えるネットワークと情報システムを設計します。システムは適切に分離され、リソースの制限は緩和されます。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
B5.c Backups	重要な機能を回復するために必要なデータおよび情報のバックアップを、アクセス可能かつ安全に保持します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.a Monitoring Coverage	モニタリングに含めるデータソースによって、重要な機能の運用に影響を及ぼす可能性のあるセキュリティイベントをタイムリーに特定することができます。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.b Securing Logs	ログデータは安全に保管し、業務上必要なアカウントにのみ読み取り権限を付与します。従業員は、合意した保存期間中にログデータの修正や削除を行う必要がないようにします。保存期間の終了後に削除します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	s3-event-notifications-enabled	Amazon S3 イベント通知により、バケットオブジェクトに対する偶発的または意図的な変更について、関連する担当者に警告できます。アラートの例としては、新しいオブジェクトの作成、オブジェクトの削除、オブジェクトの復元、オブジェクトの紛失およびレプリケートなどが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	api-gw-execution-logging-enabled	API Gateway の口グ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.c Generating Alerts	モニタリングデータに含まれる潜在的なセキュリティインシデントの証拠を確実に特定し、アラートを発します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.d Identifying Security Incidents	脅威やシステムに関する知識をもとにアラートの文脈を整理し、何らかの対応が必要なセキュリティインシデントを特定することができます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.d Identifying Security Incidents	脅威やシステムに関する知識をもとにアラートの文脈を整理し、何らかの対応が必要なセキュリティインシデントを特定することができます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.e Monitoring Tools and Skills	モニタリングスタッフのスキル、ツール、役割は、アウトソーシングされているものも含め、ガバナンスと報告要件、予想される脅威、使用する必要のあるネットワークやシステムデータの複雑さを反映したものにする必要があります。監視スタッフは、守るべき本質的な機能についての知識を備えています。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.e Monitoring Tools and Skills	モニタリングスタッフのスキル、ツール、役割は、アウトソーシングされているものも含め、ガバナンスと報告要件、予想される脅威、使用する必要のあるネットワークやシステムデータの複雑さを反映したものにする必要があります。監視スタッフは、守るべき本質的な機能についての知識を備えています。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C1.e Monitoring Tools and Skills	モニタリングスタッフのスキル、ツール、役割は、アウトソーシングされているものも含め、ガバナンスと報告要件、予想される脅威、使用する必要のあるネットワークやシステムデータの複雑さを反映したものにする必要があります。監視スタッフは、守るべき本質的な機能についての知識を備えています。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C2.a System Abnormalities for Attack Detection	システム動作の異常の例を定義することで、他の方法では特定が困難な悪意のある活動を検出する実用的な方法を提供します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
C2.a System Abnormalities for Attack Detection	システム動作の異常の例を定義することで、他の方法では特定が困難な悪意のある活動を検出する実用的な方法を提供します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
D1.c Testing and Exercising	組織は、自分たちの組織や他の組織に影響を与えた過去の事件や、脅威情報とリスクアセスメントに基づくシナリオを使用して、対応計画をテストする演習を実施します。	response-plan-exists-maintained (Process Check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。正式にドキュメント化された更新済みの対応計画を用意することで、対応する担当者がインシデントの発生中に従うべき役割、責任、プロセスを理解することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
D1.c Testing and Exercising	組織は、自分たちの組織や他の組織に影響を与えた過去の事件や、脅威情報とリスクアセスメントに基づくシナリオを使用して、対応計画をテストする演習を実施します。	response-plan-tested (Process Check)	インシデント対応と復旧計画がテスト済みであることを確認します。これにより、インシデント発生時に計画が有効であるか、ギャップや更新に対処する必要があるかどうかを理解することができます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NCSC Cyber Assesment Framework」で入手できます。

ネットワークおよびコンテンツ配信サービスの運用のベストプラクティス

このコンフォーマンスパックには、ネットワークおよびコンテンツ配信サービスに基づく AWS Config ルールが含まれています。詳細については、「 でのネットワークとコンテンツの配信 AWS」を参照してください。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Networking and Content Delivery Services」で入手できます。

NIST の「800-53 rev 4」の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するよう

には設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、NIST 800-53 と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の NIST 800-53 コントロールに関連付けられます。NIST の「800-53」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックは、Payment Card Industry Qualified Security Assessors (QSAs)、HITRUST Certified Common Security Framework Practitioners (CCSFPs)、およびさまざまな業界フレームワークのガイダンスと評価を提供することを認定されたコンプライアンスプロフェッショナルのチームである AWS Security Assurance Services LLC (AWS SAS) によって検証されました。 AWS SAS プロフェッショナルは、お客様が NIST 800-53 のサブセットに対応できるようにこのコンフォーマンスパックを設計しました。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするため	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	の自動化されたメカニズムを採用します。		少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 および Centers for Internet Security (CIS) AWS Foundations Benchmark で説明されているパスワード強度に関する要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、RequireSymbols (AWS Foundational Security Best Practices 値： true)、RequireNumbers (AWS Foundational Security Best Practices 値： true)、 MinimumPasswordLength (AWS

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (1)	組織は、情報システムアカウントの管理をサポートするための自動化されたメカニズムを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (3)	情報システムは、[Assignment: organization-defined time period (割り当て: 組織で定義された期間)] の後に非アクティブなアカウントを自動的に無効にします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloudtrail-enabled	AWS CloudTrail は、マネジメントコンソールのアクションと API コールを記録 AWS することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての から S3 バケット AWS リージョンにログファイルを配信します。さらに、AWS が新しいリージョンを作成すると、CloudTrail はそのリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (4)	情報システムは、アカウントの作成、変更、有効化、無効化、削除のアクションを自動的に監査し、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に通知します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (12)(a)	組織: a。[Assignment: organization-defined atypical use (割り当て: 組織で定義された非定型の使用)] の情報システムアカウントをモニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (12)(a)	組織: a。[Assignment: organization-defined atypical use (割り当て: 組織で定義された非定型の使用)] の情報システムアカウントをモニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 および Centers for Internet Security (CIS) AWS Foundations Benchmark で説明されているパスワード強度に関する要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、RequireSymbols (AWS Foundational Security Best Practices 値： true)、RequireNumbers (AWS Foundational Security Best Practices 値： true)、 MinimumPasswordLength (AWS

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-2 (f)	組織: f。[Assignment: organization-defined procedures or conditions (割り当て: 組織で定義された手順または条件)] に従って、情報システムアカウントを作成、有効化、変更、無効化、および削除します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	cloudtrail-enabled	AWS CloudTrail は、マネジメントコンソールのアクションと API コールを記録 AWS することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント の情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (g)	組織: g。情報システムアカウントの使用をモニタリングします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 および Centers for Internet Security (CIS) AWS Foundations Benchmark で説明されているパスワード強度に関する要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、RequireSymbols (AWS Foundational Security Best Practices 値： true)、RequireNumbers (AWS Foundational Security Best Practices 値： true)、 MinimumPasswordLength (AWS

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-2 (j)	組織: j。アカウント管理要件への準拠について、アカウントを確認します: [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)]。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	s3-account-level-public-access-blocks	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-3	情報システムは、適用されるアクセスコントロールポリシーに従い、情報およびシステムリソースへの論理的アクセスに対して、承認された認可を実施します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。Amazon VPC 内に存在するドメインは論理的に隔離されているため、パブリックエンドポイントを使用するドメインよりも多くのセキュリティレイヤーが追加されています。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	s3-account-level-public-access-blocks	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-4	情報システムは、[Assignment: organization-defined information flow control policies (割り当て: 組織で定義された情報フローの管理ポリシー)] に基づいて、システム内および相互接続されたシステム間の情報フローを制御するための承認された認可を実施します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-5c	組織: c。職務の分離をサポートするための情報システムのアクセス許可を定義します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Managemen t (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-account-level-public-access-blocks	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6	組織は、最小特権の原則を採用し、組織のミッションとビジネス機能に従って割り当てられたタスクを達成するために必要なユーザー (またはユーザーに代わるプロセス) の認可されたアクセスのみを許可します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-6 (10)	情報システムは、非特権ユーザーが特権的機能を実行して、実装されたセキュリティの保護/対策を無効化、回避、変更することを防ぎます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-17 (1)	情報システムは、リモートアクセスの方法をモニタリングおよびコントロールします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC-17 (2)	情報システムは、リモートアクセスセッションの機密性と整合性を保護するための暗号化メカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-17 (3)	情報システムは、[Assignment: organization-defined number (割り当て: 組織で定義された数)] で管理されるネットワークアクセスコントロールポイントを介して、すべてのリモートアクセスをルーティングします。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-account-level-public-access-blocks	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AC-21 (b)	組織: b。ユーザーによる情報共有と共同作業の意思決定を支援するため、[Assignment: organization-defined automated mechanisms or manual processes (割り当て: 組織で定義された自動化されたメカニズムまたは手動のプロセス)] を採用します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント の情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	cloudtrail-enabled	AWS CloudTrail は、マネジメントコンソールのアクションと API コールを記録 AWS することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての から S3 バケット AWS リージョンにログファイルを配信します。さらに、AWS が新しいリージョンを作成すると、CloudTrail はそのリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-2 (a)(d)	組織: a。情報システムが以下のイベントを監査可能であることを決定します: [Assignment: organization-defined auditable events (割り当て: 組織で定義された監査可能なイベント)]: d。以下のイベントを情報システム内で監査することを決定します。[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a (割り当て: 組織で定義された監査可能なイベント (AU-2 a で定義された監査可能なイベントのサブ集合)]。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント の情報、IP アドレス、イベント発生時刻が含まれます。
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	cloudtrail-enabled	AWS CloudTrail は、マネジメントコンソールのアクションと API コールを記録 AWS することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての から S3 バケット AWS リージョンにログファイルを配信します。さらに、AWS が新しいリージョンを作成すると、CloudTrail はそのリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-3	情報システムは、発生したイベントのタイプ、イベントの発生日時、イベントの発生場所、イベントのソース、イベントの結果、イベントに関連付けられた個人またはサブジェクトの ID を証明する情報を含む監査レコードを生成します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-6 (1)(3)	(1) 組織は、疑わしいアクティビティを調査し対応するための組織のプロセスをサポートするための監査のレビュー、分析、および報告のプロセスを統合する自動化されたメカニズムを採用します。(3) 組織は、さまざまなリポジトリ間で監査レコードを分析し相互に関連付けて、組織全体の状況認識を行います。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-7 (1)	情報システムは、[Assignment: organization-defined audit fields within audit records (割り当て: 組織で定義された監査レコード内の監査フィールド)] に基づいて、対象のイベントの監査レコードを処理する機能を提供します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-7 (1)	情報システムは、[Assignment: organization-defined audit fields within audit records (割り当て: 組織で定義された監査レコード内の監査フィールド)] に基づいて、対象のイベントの監査レコードを処理する機能を提供します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-9	情報システムは、監査情報と監査ツールを不正アクセス、変更、削除から保護します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
AU-9	情報システムは、監査情報と監査ツールを不正アクセス、変更、削除から保護します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-9 (2)	情報システムは、監査対象のシステムやコンポーネントとは物理的に異なるシステムまたはシステムコンポーネントに、監査記録 [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] をバックアップします。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
AU-11	組織は、[Assignment: organization-defined time period consistent with records retention policy (割り当て: 組織で定義された記録保持のポリシーと一致する期間)] の監査レコードを保持することで、セキュリティインシデントの事後調査をサポートするとともに、規制および組織の情報保持の要件を満たします。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント の情報、IP アドレス、イベント発生時刻が含まれます。
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	cloudtrail-enabled	AWS CloudTrail は、マネジメントコンソールのアクションと API コールを記録 AWS することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての から S3 バケット AWS リージョンにログファイルを配信します。さらに、AWS が新しいリージョンを作成すると、CloudTrail はそのリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
AU-12 (a)(c)	情報システム: a。AU-2 a.で定義された監査可能なイベントについて、[Assignment: organization-defined information system components] での監査記録の生成機能を提供します: c。AU-2 d で定義されたイベントの監査レコードを、AU-3 で定義された内容で作成します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングを裏付ける評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングをサポートする評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングをサポートする評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングをサポートする評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングをサポートする評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CA-7 (a)(b)	組織は、継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実装します。モニタリング対象の [Assignment: organization-defined metrics (割り当て: 組織で定義されたメトリクス)] の設定。モニタリングのための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] およびそれらのモニタリングをサポートする評価のための [Assignment: organization-defined frequencies (割り当て: 組織で定義された頻度)] の確立。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-2	組織は、情報システムの現在のベースラインの設定を開発し、ドキュメント化し、設定を管理して維持します。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることを確認することで AWS CloudTrail、 AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョン AWS CloudTrail での の有効化が含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-7 (a)	組織: a。重要な機能のみを提供するように情報システムを設定します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-7 (a)	組織: a。重要な機能のみを提供するように情報システムを設定します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-8 (1)	組織は、コンポーネントのインストール、削除、および情報システムの更新において不可欠な部分である情報システムコンポーネントのインベントリを更新します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-8 (3)(a)	組織: a。自動化されたメカニズム [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] を採用して、情報システム内に存在する未許可のハードウェア、ソフトウェア、ファームウェアコンポーネントを検出します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-8 (3)(a)	組織: a。自動化されたメカニズム [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] を採用して、情報システム内に存在する未許可のハードウェア、ソフトウェア、ファームウェアコンポーネントを検出します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CM-8 (3)(a)	組織: a。自動化されたメカニズム [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] を採用して、情報システム内に存在する未許可のハードウェア、ソフトウェア、ファームウェアコンポーネントを検出します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CP-9 (b)	組織: b。情報システムの [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] に含まれるシステムレベルの情報のバックアップを実行します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-9 (b)	組織: b。情報システムの [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] に含まれるシステムレベルの情報のバックアップを実行します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-9 (b)	組織: b。情報システムの [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] に含まれるシステムレベルの情報のバックアップを実行します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-9 (b)	組織: b。情報システムの [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] に含まれるシステムレベルの情報のバックアップを実行します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-9 (b)	組織: b。情報システムの [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] に含まれるシステムレベルの情報のバックアップを実行します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-9 (b)	組織: b。情報システムの [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] に含まれるシステムレベルの情報のバックアップを実行します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-9 (b)	組織: b。情報システムの [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] に含まれるシステムレベルの情報のバックアップを実行します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-9 (b)	組織: b。情報システムの [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] に含まれるシステムレベルの情報のバックアップを実行します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
CP-10	組織は、中断、侵害、障害の発生後、情報システムを既知の状態に復旧し再構成します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IA-2	情報システムは、組織のユーザー (または組織のユーザーに代わって実行するプロセス) を一意に識別し認証します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 および Centers for Internet Security (CIS) AWS Foundations Benchmark で説明されているパスワード強度に関する要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、RequireSymbols (AWS Foundational Security Best Practices 値： true)、RequireNumbers (AWS Foundational Security Best Practices 値： true)、 MinimumPasswordLength (AWS

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IA-2(1)(11)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(11) 情報システムには、特権アカウントと非特権アカウントへのリモートアクセスのための多要素認証を実装します。その際、要素の 1 つはアクセスを取得するシステムとは別のデバイスによって提供され、その装置が [Assignment: organization-defined strength of mechanism requirement] を満たすようにします。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IA-2(1)(11)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(11) 情報システムには、特権アカウントと非特権アカウントへのリモートアクセスのための多要素認証を実装します。その際、要素の 1 つはアクセスを取得するシステムとは別のデバイスによって提供され、その装置が [Assignment: organization-defined strength of mechanism requirement] を満たすようにします。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IA-2(1)(2)(11)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(2) 情報システムは、非特権アカウントへのネットワークアクセスのための多要素認証を実装します。(11) 情報システムには、特権アカウントと非特権アカウントへのリモートアクセスのための多要素認証を実装します。その際、要素の 1 つはアクセスを取得するシステムとは別のデバイスによって提供され、その装置が [Assignment: organization-defined strength of mechanism requirement] を満たすようにします。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IA-2(1)(2)(11)	(1) 情報システムは、権限のあるアカウントへのネットワークアクセスのための多要素認証を実装します。(2) 情報システムは、非特権アカウントへのネットワークアクセスのための多要素認証を実装します。(11) 情報システムには、特権アカウントと非特権アカウントへのリモートアクセスのための多要素認証を実装します。その際、要素の 1 つはアクセスを取得するシステムとは別のデバイスによって提供され、その装置が [Assignment: organization-defined strength of mechanism requirement] を満たすようにします。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IA-5 (1)(a)(d)(e)	パスワードベースの認証のための情報システム: a。[Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type (割り当て: 組織で定義された大文字と小文字の区別、文字数、大文字、小文字、数字、特殊文字の組み合わせに関する、各タイプの最小要件を含む要件)] のパスワードの複雑さを最小限に抑えます: d。[Assignment: organization- defined numbers for lifetime minimum, lifetime maximum (割り当て: 組織で定義されたライフタイムの最小および最大の数値)] のパスワードの最小および最大有効期間の制限を適用しま	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 および Centers for Internet Security (CIS) AWS Foundations Benchmark で説明されているパスワード強度に関する要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、RequireSymbols (AWS Foundational Security Best Practices 値： true)、RequireNumbers (AWS Foundational Security Best Practices 値： true)、 MinimumPasswordLength (AWS

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	す: e。[Assignment: organization-defined number (割り当て: 組織で定義された数)] 世代のパスワードの再利用を禁止します。		基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IA-5 (4)	組織は、自動化されたツールを使用して、パスワード認証システムに [Assignment: organization-defined requirements (割り当て: 組織で定義された要件)] を満たす十分な強度があるかどうかを判断します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 および Centers for Internet Security (CIS) AWS Foundations Benchmark で説明されているパスワード強度に関する要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、RequireSymbols (AWS Foundational Security Best Practices 値： true)、RequireNumbers (AWS Foundational Security Best Practices 値： true)、 MinimumPasswordLength (AWS

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA-5 (7)	組織は、暗号化されていない静的オーセンティケーターが、アプリケーションやアクセススクリプトに埋め込まれたり、ファンクションキーに割り当てられたりしていないことを確認します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IR-4 (1)	組織は、インシデント対応プロセスをサポートするための自動化されたメカニズムを採用します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IR-6 (1)	組織は、セキュリティインシデントの報告をサポートするための自動化されたメカニズムを採用します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
IR-7 (1)	組織は、インシデント対応に関連する情報およびサポートの可用性を高めるための自動化されたメカニズムを採用します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
RA-5	組織: a。情報システムおよびホストされているアプリケーションの脆弱性をスキャンし [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process (割り当て: 組織で定義された頻度および/またはプロセスに従ったランダムな頻度)]、システム/アプリケーションに影響を与える可能性のある新たな脆弱性が特定され、報告された場合にもスキャンします: b。ツール間の相互運用性を促進し、脆弱性管理プロセスの一部を自動化するために、以下の標準を使用した脆弱性スキャンツールおよびテクノロジーを採用します: 1。プラットフォーム、ソフトウェアの欠陥、不適切な構成を列挙します: 2。チェックリストとテスト手順	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	のフォーマット: および 3。脆弱性による影響の測定: c。脆弱性スキャンレポートとセキュリティコントロール評価の結果を分析します: d。リスクの組織的評価に従って、正当な脆弱性を修正します: [Assignment: organization-defined response times (割り当て: 組織で定義された応答時間)]: および e。脆弱性スキャンプロセスおよびセキュリティコントロール評価から取得した情報を [Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] と共有し、他の情報システムにおける同様の脆弱性 (システム的な弱点や欠陥) を排除します。		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
RA-5	組織: a。情報システムおよびホストされているアプリケーションの脆弱性をスキャンし [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process (割り当て: 組織で定義された頻度および/またはプロセスに従ったランダムな頻度)]、システム/アプリケーションに影響を与える可能性のある新たな脆弱性が特定され、報告された場合にもスキャンします: b。ツール間の相互運用性を促進し、脆弱性管理プロセスの一部を自動化するために、以下の標準を使用した脆弱性スキャンツールおよびテクノロジーを採用します: 1。プラットフォーム、ソフトウェアの欠陥、不適切な構成を列挙します: 2。チェックリストとテスト手順	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	のフォーマット: および 3。脆弱性による影響の測定: c。脆弱性スキャンレポートとセキュリティコントロール評価の結果を分析します: d。リスクの組織的評価に従って、正当な脆弱性を修正します: [Assignment: organization-defined response times (割り当て: 組織で定義された応答時間)]: および e。脆弱性スキャンプロセスおよびセキュリティコントロール評価から取得した情報を [Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] と共有し、他の情報システムにおける同様の脆弱性 (システム的な弱点や欠陥) を排除します。		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SA-3 (a)	組織: a。情報セキュリティの考慮事項が組み込まれた [Assignment: organization-defined system development life cycle (割り当て: 組織で定義されたシステム開発のライフサイクル)] を使用して、情報システムを管理します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SA-3 (a)	組織: a。情報セキュリティの考慮事項が組み込まれた [Assignment: organization-defined system development life cycle (割り当て: 組織で定義されたシステム開発のライフサイクル)] を使用して、情報システムを管理します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SA-3 (a)	組織: a。情報セキュリティの考慮事項が組み込まれた [Assignment: organization-defined system development life cycle (割り当て: 組織で定義されたシステム開発のライフサイクル)] を使用して、情報システムを管理します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、 AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、またはサービスの実行中に設定管理を行います [選択 (1 つまたは複数): design; development; implementation; operation]: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	をドキュメント化する: および e。システム、コンポーネント、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、またはサービスの実行中に設定管理を行います [選択 (1 つまたは複数): design; development; implementation; operation]: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	をドキュメント化する: および e。システム、コンポーネント、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、またはサービスの実行中に設定管理を行います [選択 (1 つまたは複数): design; development; implementation; operation]: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	をドキュメント化する: および e。システム、コンポーネント、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SA-10	組織は、情報システム、システムコンポーネント、情報システムサービスのデベロッパーに以下を要求します: a。システム、コンポーネント、またはサービスの実行中に設定管理を行います [選択 (1 つまたは複数): design; development; implementation; operation]: b。[Assignment: organization-defined configuration items under configuration management (割り当て: 組織で定義された設定管理における設定項目)] への変更の整合性をドキュメント化し、管理および制御する: c。システム、コンポーネント、サービスには組織が承認した変更のみを実装する: d。システム、コンポーネント、サービスに対する承認された変更と、それらの変更による潜在的なセキュリティへの影響	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
	をドキュメント化する: および e。システム、コンポーネント、サービス内のセキュリティの欠陥の解決状況を追跡し、結果を [Assignment: organization-defined personnel (割り当て: 組織で定義される担当者)] に報告します。		
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-2	情報システムは、ユーザー機能 (ユーザーインターフェイスサービスを含む) を情報システムの管理機能から分離します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-4	情報システムは、共有システムリソースから不正で意図しない情報転送を防止します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-5	情報システムは、[Assignment: organization-defined security safeguards (割り当て: 組織で定義されたセキュリティの安全対策)] を採用することで、以下のタイプのサービス拒否攻撃の影響保護し、またはその影響を制限します。[Assignment: organization-defined types of denial of service attacks or references to sources for such information (割り当て: 組織で定義されたタイプのサービス拒否攻撃またはそれらの情報のソースの参照]。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。Amazon VPC 内に存在するドメインは論理的に隔離されているため、パブリックエンドポイントを使用するドメインよりも多くのセキュリティレイヤーが追加されています。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	s3-account-level-public-access-blocks	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7	情報システム: a。システムの外部境界およびシステム内の主要な内部境界での通信をモニタリングおよびコントロールします: b 組織内のネットワークから分離された [Selection: physically; logically] でパブリックにアクセス可能なシステムコンポーネントのためのサブネットワークを採用します: および c。外部のネットワークや情報システムへの接続は、組織のセキュリティアーキテクチャに従って配置された境界保護装置で構成される管理されたインターフェイスを通じてのみ行います。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。Amazon VPC 内に存在するドメインは論理的に隔離されているため、パブリックエンドポイントを使用するドメインよりも多くのセキュリティレイヤーが追加されています。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-account-level-public-access-blocks	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-7 (3)	組織は、情報システムへの外部ネットワーク接続の数を制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8	情報システムは、転送される情報の [選択 (1 つまたは複数): confidentiality; integrity] を保護します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の [選択 (1 つまたは複数): confidentiality; integrity] を保護します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8	情報システムは、転送される情報の [選択 (1 つまたは複数): confidentiality; integrity] を保護します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の [選択 (1 つまたは複数): confidentiality; integrity] を保護します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8	情報システムは、転送される情報の [選択 (1 つまたは複数): confidentiality; integrity] を保護します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	情報システムは、転送される情報の [選択 (1 つまたは複数): confidentiality; integrity] を保護します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8	情報システムは、転送される情報の [選択 (1 つまたは複数): confidentiality; integrity] を保護します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-8 (1)	情報システムでは、[Assignment: organization-defined alternative physical safeguards (割り当て: 組織で定義された代替の物理的な安全対策)] によって保護されている場合を除き、転送中の [選択 (1 つまたは複数): prevent unauthorized disclosure of information; detect changes to information (選択 (1 つ以上): 情報の不正開示の防止、情報の変更の検出)] のための暗号メカニズムを実装します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC-12	組織は、[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] に従って、情報システム内で使用される必要な暗号化の暗号化キーを確立および管理します。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-12	組織は、[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] に従って、情報システム内で使用される必要な暗号化の暗号化キーを確立および管理します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-12	組織は、[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] に従って、情報システム内で使用される必要な暗号化の暗号化キーを確立および管理します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、[Assignment: organization-defined cryptographic uses and type of cryptography required for each use (割り当て: 組織で定義された暗号化の使用と、各用途に必要な暗号化のタイプ)] を実装します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-13	情報システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従って、FIPS で検証された、または NSA で承認された暗号化を実装します。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
SC-23	情報システムは、通信セッションの信頼性を保護します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-23	情報システムは、通信セッションの信頼性を保護します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23	情報システムは、通信セッションの信頼性を保護します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	情報システムは、[Assignment: organization-defined information at rest (割り当て: 組織で定義された保管時の情報)] の [選択 (1 つまたは複数): confidentiality; integrity (選択 (1 つ以上): 機密性、完全性)] を保護します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-36	組織は、[Assignment: organization-defined processing and storage (割り当て: 組織で定義された処理とストレージ)] を、複数の物理的な場所に配布します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SC-36	組織は、[Assignment: organization-defined processing and storage (割り当て: 組織で定義された処理とストレージ)] を、複数の物理的な場所に配布します。	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
SC-36	組織は、[Assignment: organization-defined processing and storage (割り当て: 組織で定義された処理とストレージ)] を、複数の物理的な場所に配布します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
SI-2 (2)	組織は、自動化されたメカニズム [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] を使用して、情報システムコンポーネントでの欠陥の修正に関する状態を判断します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-2 (2)	組織は、自動化されたメカニズム [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] を使用して、情報システムコンポーネントでの欠陥の修正に関する状態を判断します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-2 (2)	組織は、自動化されたメカニズム [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] を使用して、情報システムコンポーネントでの欠陥の修正に関する状態を判断します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (1)	組織は、個々の侵入検知ツールを情報システム全体の侵入検知システムに接続し、設定します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
SI-4 (2)	組織は、ほぼリアルタイムのイベント分析をサポートするための自動化されたツールを採用します。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (4)	情報システムは、異常なまたは許可されていない活動または状態について、インバウンドおよびアウトバウンドの通信トラフィック [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] をモニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (4)	情報システムは、異常なまたは許可されていない活動または状態について、インバウンドおよびアウトバウンドの通信トラフィック [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] をモニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (4)	情報システムは、異常なまたは許可されていない活動または状態について、インバウンドおよびアウトバウンドの通信トラフィック [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] をモニタリングします。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (4)	情報システムは、異常なまたは許可されていない活動または状態について、インバウンドおよびアウトバウンドの通信トラフィック [Assignment: organization-defined frequency (割り当て: 組織で定義された頻度)] をモニタリングします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (5)	情報システムは、以下の侵害または潜在的な侵害の兆候が発生した場合、[Assignment: organization-defined personnel or roles (割り当て: 組織で定義された人員またはロール)] に [Assignment: organization- defined compromise indicators (割り当て: 組織で定義された妥協の指標)] のアラートを送信します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (16)	組織は、情報システム全体で採用されているモニタリングツールからの情報を相関させます。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-4 (a)(b)(c)	組織: a。情報システムをモニタリングして、以下を検出します: 1。[Assignment: organization-defined monitoring objectives] に準拠した攻撃と潜在的な攻撃の指標:　2。未許可のローカル、ネットワーク、リモート接続: b。[Assignment: organization-defined techniques and methods (割り当て: 組織で定義された技術と方法] を通じて、情報システムの不正使用を特定します: c。モニタリング装置のデプロイ: (i) 組織が決定した重要な情報を収集するため、情報システム内に戦略的にデプロイし、(ii) 組織が関心を持つ特定のタイプのトランザクションを追跡するため、システム内のアドホックな場所にデプロイします。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-7	組織は、[Assignment: organization-defined software, firmware, and information (割り当て: 組織で定義されたソフトウェア、ファームウェア、情報)] に対する不正な変更を検出するための整合性検証ツールを採用します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性を確認します。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-7 (1)	情報システムは、[Assignment: organization-defined software, firmware, and information 割り当て: 組織で定義されたソフトウェア、ファームウェア、情報)] と [Assignment: organization-defined transitional states or security-relevant events (割り当て: 組織で定義された移行ステータスまたはセキュリティ関連イベント)]、[Assignment: organization- defined frequency (割り当て: 組織で定義された頻度)] での [選択 (1 つまたは複数): at startup (選択 (1 つ以上): 起動時)] との整合性のチェックを行います。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-7 (1)	情報システムは、[Assignment: organization-defined software, firmware, and information 割り当て: 組織で定義されたソフトウェア、ファームウェア、情報)] と [Assignment: organization-defined transitional states or security-relevant events (割り当て: 組織で定義された移行ステータスまたはセキュリティ関連イベント)]、[Assignment: organization- defined frequency (割り当て: 組織で定義された頻度)] での [選択 (1 つまたは複数): at startup (選択 (1 つ以上): 起動時)] との整合性のチェックを行います。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-7 (1)	情報システムは、[Assignment: organization-defined software, firmware, and information 割り当て: 組織で定義されたソフトウェア、ファームウェア、情報)] と [Assignment: organization-defined transitional states or security-relevant events (割り当て: 組織で定義された移行ステータスまたはセキュリティ関連イベント)]、[Assignment: organization- defined frequency (割り当て: 組織で定義された頻度)] での [選択 (1 つまたは複数): at startup (選択 (1 つ以上): 起動時)] との整合性のチェックを行います。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性を確認します。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS Config ルール	ガイダンス
SI-12	組織は、適用される連邦法、大統領令、指令、ポリシー、規制、基準、運用要件に従って、情報システム内の情報およびシステムから出力される情報を処理および保持します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NIST 800-53 rev 4」で入手できます。

NIST の「800-53 rev 5」の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、NIST 800-53 と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の NIST 800-53 コントロールに関連付けられます。NIST の「800-53」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	アカウント管理 | 自動監査アクション	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
AC-2 (4)	アカウント管理 | 自動監査アクション	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信し

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ます。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
AC-2 (4)	アカウント管理 | 自動監査アクション	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	アカウント管理 | 自動監査アクション	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AC-2 (4)	アカウント管理 | 自動監査アクション	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	アカウント管理 | 自動監査アクション	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AC-2 (4)	アカウント管理 | 自動監査アクション	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	アカウント管理 | 自動監査アクション	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2 (4)	アカウント管理 | 自動監査アクション	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2(12)	アカウント管理 | 非定型使用のアカウントモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウント管理	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-2	アカウント管理	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウント管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウント管理	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウント管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウント管理	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-2	アカウント管理	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3(15)	アクセス権の実施 | 任意および強制的なアクセス制御	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager シークレットのローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
AC-3	アクセスの実施	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
AC-3	アクセスの実施	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。
AC-3	アクセスの実施	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-3	アクセスの実施	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
AC-3	アクセスの実施	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-3	アクセスの実施	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-3	アクセスの実施	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-3	アクセスの実施	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-3	アクセスの実施	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-3	アクセスの実施	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-4(26)	情報フローの実施 | 監査フィルタリングアクション	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5	職務の分離	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。
AC-5	職務の分離	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5	職務の分離	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5	職務の分離	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5	職務の分離	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-5	職務の分離	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC-6(2)	最小特権 | 非セキュリティ機能に対する非特権アクセス	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(2)	最小特権 | 非セキュリティ機能に対する非特権アクセス	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(2)	最小特権 | 非セキュリティ機能に対する非特権アクセス	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(3)	最小特権 | 特権コマンドへのネットワークアクセス	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
AC-6(3)	最小特権 | 特権コマンドへのネットワークアクセス	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(3)	最小特権 | 特権コマンドへのネットワークアクセス	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(3)	最小特権 | 特権コマンドへのネットワークアクセス	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(3)	最小特権 | 特権コマンドへのネットワークアクセス	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(3)	最小特権 | 特権コマンドへのネットワークアクセス	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
AC-6(9)	最小特権 | 特権を持つ機能の使用についてのログ	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	最小特権 | 特権を持つ機能の使用についてのログ	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	最小特権 | 特権を持つ機能の使用についてのログ	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
AC-6(9)	最小特権 | 特権を持つ機能の使用についてのログ	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	最小特権 | 特権を持つ機能の使用についてのログ	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
AC-6(9)	最小特権 | 特権を持つ機能の使用についてのログ	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	最小特権 | 特権を持つ機能の使用についてのログ	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	最小特権 | 特権を持つ機能の使用についてのログ	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6(9)	最小特権 | 特権を持つ機能の使用についてのログ	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 (10)	最小特権 | 非特権ユーザーによる特権関数の実行の禁止	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
AC-6 (10)	最小特権 | 非特権ユーザーによる特権関数の実行の禁止	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-6 (10)	最小特権 | 非特権ユーザーによる特権関数の実行の禁止	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (2)	リモートアクセス | 暗号化による機密性と整合性の保護	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
AC-17 (2)	リモートアクセス | 暗号化による機密性と整合性の保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (2)	リモートアクセス | 暗号化による機密性と整合性の保護	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
AC-17 (2)	リモートアクセス | 暗号化による機密性と整合性の保護	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
AC-17 (2)	リモートアクセス | 暗号化による機密性と整合性の保護	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-17 (2)	リモートアクセス | 暗号化による機密性と整合性の保護	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
AC-17 (2)	リモートアクセス | 暗号化による機密性と整合性の保護	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
AC-21	情報共有	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-21	情報共有	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
AC-21	情報共有	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
AC-21	情報共有	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
AC-21	情報共有	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
AC-21	情報共有	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AC-21	情報共有	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	イベントログ	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	イベントログ	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	イベントログ	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
AU-2	イベントログ	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	イベントログ	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-2	イベントログ	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	イベントログ	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-2	イベントログ	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	イベントログ	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-2	イベントログ	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	イベントログ	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	イベントログ	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-2	イベントログ	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-3	監査記録の内容	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-3	監査記録の内容	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-3	監査記録の内容	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-3	監査記録の内容	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-3	監査記録の内容	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-6(1)	監査記録のレビュー、分析、および報告 | 自動プロセスの統合	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(1)	監査記録のレビュー、分析、および報告 | 自動プロセスの統合	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(1)	監査記録のレビュー、分析、および報告 | 自動プロセスの統合	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(1)	監査記録のレビュー、分析、および報告 | 自動プロセスの統合	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(3)	監査記録のレビュー、分析、および報告 | 監査記録リポジトリの相互関連付け	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(4)	監査記録のレビュー、分析、および報告 | 集約型レビューと分析	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
AU-6(5)	監査記録のレビュー、分析、および報告 | 監査記録の統合分析	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(5)	監査記録のレビュー、分析、および報告 | 監査記録の統合分析	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(5)	監査記録のレビュー、分析、および報告 | 監査記録の統合分析	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-6(5)	監査記録のレビュー、分析、および報告 | 監査記録の統合分析	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-7 (1)	監査の削減と報告の生成 | 自動処理	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-9 (2)	監査情報の保護 | 分離された物理システムまたはコンポーネントに保存	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9 (2)	監査情報の保護 | 分離された物理システムまたはコンポーネントに保存	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9 (2)	監査情報の保護 | 分離された物理システムまたはコンポーネントに保存	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
AU-9(7)	監査情報の保護 | さまざまなオペレーティングシステムのコンポーネントに保存	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9	監査情報の保護	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
AU-9	監査情報の保護	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9	監査情報の保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
AU-9	監査情報の保護	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-9	監査情報の保護	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
AU-10	非否認	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-10	非否認	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-10	非否認	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
AU-10	非否認	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-10	非否認	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-10	非否認	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-10	非否認	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-10	非否認	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-10	非否認	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-10	非否認	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-10	非否認	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-10	非否認	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
AU-12	監査記録の生成	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
AU-12	監査記録の生成	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
AU-12	監査記録の生成	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-12	監査記録の生成	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
AU-14(1)	セッションの監査 | システム起動	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
CA-7	継続的なモニタリング	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
CA-7	継続的なモニタリング	s3-event-notifications-enabled	Amazon S3 イベント通知により、バケットオブジェクトに対する偶発的または意図的な変更について、関連する担当者に警告できます。アラートの例としては、新しいオブジェクトの作成、オブジェクトの削除、オブジェクトの復元、オブジェクトの紛失およびレプリケートなどが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
CA-7	継続的なモニタリング	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
CA-7	継続的なモニタリング	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
CA-7	継続的なモニタリング	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CA-7	継続的なモニタリング	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-7	継続的なモニタリング	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	rds-instance-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Relational Database Service (Amazon RDS) データベースインスタンスのアタックサーフェスを減らすことができます。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	redshift-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Redshift クラスターのアタックサーフェスを減らすことができます。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
CA-9(1)	内部システムの接続 | コンプライアンスチェック	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CA-9(1)	内部システムの接続 | コンプライアンスチェック	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2(2)	ベースラインの設定 | 正確性と最新性のためのオートメーションサポート	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2(2)	ベースラインの設定 | 正確性と最新性のためのオートメーションサポート	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
CM-2(2)	ベースラインの設定 | 正確性と最新性のためのオートメーションサポート	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2(2)	ベースラインの設定 | 正確性と最新性のためのオートメーションサポート	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
CM-2(2)	ベースラインの設定 | 正確性と最新性のためのオートメーションサポート	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2(2)	ベースラインの設定 | 正確性と最新性のためのオートメーションサポート	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
CM-2	ベースラインの設定	rds-instance-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Relational Database Service (Amazon RDS) データベースインスタンスのアタックサーフェスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
CM-2	ベースラインの設定	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
CM-2	ベースラインの設定	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-2	ベースラインの設定	redshift-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Redshift クラスターのアタックサーフェスを減らすことができます。
CM-2	ベースラインの設定	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。
CM-3(6)	設定変更の管理 | 暗号化の管理	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CM-3(6)	設定変更の管理 | 暗号化の管理	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CM-3(6)	設定変更の管理 | 暗号化の管理	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CM-3(6)	設定変更の管理 | 暗号化の管理	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CM-3(6)	設定変更の管理 | 暗号化の管理	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
CM-3(6)	設定変更の管理 | 暗号化の管理	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
CM-3(6)	設定変更の管理 | 暗号化の管理	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
CM-3(6)	設定変更の管理 | 暗号化の管理	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CM-3(6)	設定変更の管理 | 暗号化の管理	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3(6)	設定変更の管理 | 暗号化の管理	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
CM-3(6)	設定変更の管理 | 暗号化の管理	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-3	設定変更の管理	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
CM-3	設定変更の管理	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-7	最小の機能	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
CM-7	最小の機能	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-7	最小の機能	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (1)	システムコンポーネントのインベントリ | インストール中あるいは削除中の更新	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8 (1)	システムコンポーネントのインベントリ | インストール中あるいは削除中の更新	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8(2)	システムコンポーネントのインベントリ | 自動化されたメンテナンス	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8(3)	システムコンポーネントのインベントリ | 非認証コンポーネントの自動検出	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8(3)	システムコンポーネントのインベントリ | 非認証コンポーネントの自動検出	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8(3)	システムコンポーネントのインベントリ | 非認証コンポーネントの自動検出	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
CM-8(3)	システムコンポーネントのインベントリ | 非認証コンポーネントの自動検出	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8	システムコンポーネントのインベントリ	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CM-8	システムコンポーネントのインベントリ	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-2(2)	緊急時対応計画 | 容量計画	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-2(2)	緊急時対応計画 | 容量計画	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(1)	代替のストレージサイト | プライマリサイトからの分離	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(1)	代替のストレージサイト | プライマリサイトからの分離	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(1)	代替のストレージサイト | プライマリサイトからの分離	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(1)	代替のストレージサイト | プライマリサイトからの分離	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(1)	代替のストレージサイト | プライマリサイトからの分離	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(1)	代替のストレージサイト | プライマリサイトからの分離	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-6(1)	代替のストレージサイト | プライマリサイトからの分離	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(1)	代替のストレージサイト | プライマリサイトからの分離	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6(2)	代替のストレージサイト | 目標復旧時間と目標復旧ポイント	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6	代替のストレージサイト	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6	代替のストレージサイト	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6	代替のストレージサイト	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6	代替のストレージサイト	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6	代替のストレージサイト	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6	代替のストレージサイト	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
CP-6	代替のストレージサイト	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-6	代替のストレージサイト	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
CP-9	システムバックアップ	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
CP-9	システムバックアップ	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-9	システムバックアップ	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
CP-10	システムの復旧と再構築	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
CP-10	システムの復旧と再構築	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
CP-10	システムの復旧と再構築	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CP-10	システムの復旧と再構築	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	身分証明書と認証 (組織のユーザー) | 特権アカウントへの多要素認証	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	身分証明書と認証 (組織のユーザー) | 特権アカウントへの多要素認証	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	身分証明書と認証 (組織のユーザー) | 特権アカウントへの多要素認証	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2 (1)	身分証明書と認証 (組織のユーザー) | 特権アカウントへの多要素認証	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(2)	身分証明書と認証 (組織のユーザー) | 非特権アカウントへの多要素認証	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(2)	身分証明書と認証 (組織のユーザー) | 非特権アカウントへの多要素認証	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(2)	身分証明書と認証 (組織のユーザー) | 非特権アカウントへの多要素認証	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(2)	身分証明書と認証 (組織のユーザー) | 非特権アカウントへの多要素認証	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(6)	身分証明書と認証 (組織のユーザー) | アカウントへのアクセス – 個別のデバイス	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(6)	身分証明書と認証 (組織のユーザー) | アカウントへのアクセス – 個別のデバイス	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(6)	身分証明書と認証 (組織のユーザー) | アカウントへのアクセス – 個別のデバイス	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(6)	身分証明書と認証 (組織のユーザー) | アカウントへのアクセス – 個別のデバイス	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(8)	身分証明書と認証 (組織のユーザー) | アカウントへのアクセス – リプレイへの耐性	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(8)	身分証明書と認証 (組織のユーザー) | アカウントへのアクセス – リプレイへの耐性	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(8)	身分証明書と認証 (組織のユーザー) | アカウントへのアクセス – リプレイへの耐性	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-2(8)	身分証明書と認証 (組織のユーザー) | アカウントへのアクセス – リプレイへの耐性	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
IA-5(1)	Authenticator の管理 | パスワードベースの認証	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5(1)	Authenticator の管理 | パスワードベースの認証	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
IA-5(1)	Authenticator の管理 | パスワードベースの認証	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
IA-5(1)	Authenticator の管理 | パスワードベースの認証	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5(1)	Authenticator の管理 | パスワードベースの認証	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
IA-5(1)	Authenticator の管理 | パスワードベースの認証	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5(1)	Authenticator の管理 | パスワードベースの認証	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
IA-5(1)	Authenticator の管理 | パスワードベースの認証	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IA-5 (7)	Authenticator の管理 | 暗号化されていない静的認証システムが埋め込まれていない	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4 (1)	インシデント処理 | 自動化されたインシデント処理プロセス	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
IR-4(5)	インシデント処理 | システムの自動無効化	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RA-3(4)	リスク評価 | 予測サイバー分析	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3	システム開発のライフサイクル	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-3	システム開発のライフサイクル	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-8(19)	セキュリティとプライバシーエンジニアリングの原則 | 継続的保護	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-8(21)	セキュリティとプライバシーエンジニアリングの原則 | 自己分析	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-8(22)	セキュリティとプライバシーエンジニアリングの原則 | 説明責任とトレーサビリティ	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-8(25)	セキュリティとプライバシーエンジニアリングの原則 | 経済的なセキュリティ	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-11(1)	開発者のテストと評価 | 静的コード分析	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-11(6)	開発者のテストと評価 | 攻撃領域のレビュー	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-15(2)	開発プロセス、標準、ツール | セキュリティとプライバシーの追跡ツール	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-15(2)	開発プロセス、標準、ツール | セキュリティとプライバシーの追跡ツール	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-15(8)	開発プロセス、標準、ツール | 脅威と脆弱性の情報の再利用	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SA-15(8)	開発プロセス、標準、ツール | 脅威と脆弱性の情報の再利用	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(1)	サービス拒否からの保護 | 他のシステムを攻撃する能力の制限	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、および冗長性	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5(3)	サービス拒否からの保護 | 検出と監視	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-5	サービス拒否からの保護	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
SC-7 (3)	境界の保護 | アクセスポイント	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7 (3)	境界の保護 | アクセスポイント	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC-7 (3)	境界の保護 | アクセスポイント	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7 (3)	境界の保護 | アクセスポイント	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC-7 (3)	境界の保護 | アクセスポイント	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7 (3)	境界の保護 | アクセスポイント	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7 (3)	境界の保護 | アクセスポイント	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(4)	境界の保護 | 外部のテレコミュニケーションサービス	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(5)	境界の保護 | デフォルトによる拒否 — 例外による許可	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(5)	境界の保護 | デフォルトによる拒否 — 例外による許可	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(5)	境界の保護 | デフォルトによる拒否 — 例外による許可	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(5)	境界の保護 | デフォルトによる拒否 — 例外による許可	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(9)	境界の保護 | 脅威となる送信通信トラフィックの制限	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。
SC-7(10)	境界の保護 | 漏洩防止	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
SC-7(10)	境界の保護 | 漏洩防止	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
SC-7(10)	境界の保護 | 漏洩防止	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
SC-7(10)	境界の保護 | 漏洩防止	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
SC-7(10)	境界の保護 | 漏洩防止	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
SC-7(10)	境界の保護 | 漏洩防止	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-7(10)	境界の保護 | 漏洩防止	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(10)	境界の保護 | 漏洩防止	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
SC-7(10)	境界の保護 | 漏洩防止	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(11)	境界の保護 | 着信通信トラフィックの制限	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(16)	境界の保護 | システムコンポーネントの検出を防ぐ	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
SC-7(21)	境界の保護 | システムコンポーネントの隔離	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7(21)	境界の保護 | システムコンポーネントの隔離	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC-7(21)	境界の保護 | システムコンポーネントの隔離	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7(21)	境界の保護 | システムコンポーネントの隔離	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC-7(21)	境界の保護 | システムコンポーネントの隔離	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7(21)	境界の保護 | システムコンポーネントの隔離	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7(21)	境界の保護 | システムコンポーネントの隔離	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
SC-7	境界保護	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7	境界保護	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
SC-7	境界保護	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
SC-7	境界保護	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
SC-7	境界保護	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
SC-7	境界保護	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-7	境界保護	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8 (1)	伝送の機密性と完全性 | 暗号化による保護	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8(2)	伝送の機密性と整合性 | 伝送前および送信後の処理	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	伝送の機密性と整合性	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	伝送の機密性と整合性	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	伝送の機密性と整合性	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	伝送の機密性と整合性	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	伝送の機密性と整合性	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	伝送の機密性と整合性	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	伝送の機密性と整合性	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
SC-8	伝送の機密性と整合性	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-8	伝送の機密性と整合性	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-8	伝送の機密性と整合性	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-12(2)	暗号化キーの確立と管理 | 対称キー	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12(2)	暗号化キーの確立と管理 | 対称キー	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
SC-12(3)	暗号化キーの確立と管理 | 非対称キー	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12(3)	暗号化キーの確立と管理 | 非対称キー	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-12(3)	暗号化キーの確立と管理 | 非対称キー	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12(3)	暗号化キーの確立と管理 | 非対称キー	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-12(3)	暗号化キーの確立と管理 | 非対称キー	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12(3)	暗号化キーの確立と管理 | 非対称キー	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC-12(3)	暗号化キーの確立と管理 | 非対称キー	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-12	暗号化キーの確立と管理	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。
SC-12	暗号化キーの確立と管理	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
SC-13	暗号化による保護	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
SC-13	暗号化による保護	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-13	暗号化による保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
SC-13	暗号化による保護	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
SC-13	暗号化による保護	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-13	暗号化による保護	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-13	暗号化による保護	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-13	暗号化による保護	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
SC-13	暗号化による保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
SC-13	暗号化による保護	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
SC-13	暗号化による保護	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC-13	暗号化による保護	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
SC-13	暗号化による保護	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-13	暗号化による保護	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
SC-13	暗号化による保護	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-13	暗号化による保護	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-13	暗号化による保護	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23(3)	セッションの認証性 | システムによって生成される一意のセッション識別子	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23(3)	セッションの認証性 | システムによって生成される一意のセッション識別子	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23(3)	セッションの認証性 | システムによって生成される一意のセッション識別子	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
SC-23(3)	セッションの認証性 | システムによって生成される一意のセッション識別子	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23(3)	セッションの認証性 | システムによって生成される一意のセッション識別子	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23(3)	セッションの認証性 | システムによって生成される一意のセッション識別子	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23(3)	セッションの認証性 | システムによって生成される一意のセッション識別子	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC-23(3)	セッションの認証性 | システムによって生成される一意のセッション識別子	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23(3)	セッションの認証性 | システムによって生成される一意のセッション識別子	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23(5)	セッションの認証性 | 許可された認証機関	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23(5)	セッションの認証性 | 許可された認証機関	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC-23	セッションの認証性	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	セッションの認証性	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23	セッションの認証性	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	セッションの認証性	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-23	セッションの認証性	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	セッションの認証性	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
SC-23	セッションの認証性	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	セッションの認証性	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SC-23	セッションの認証性	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-23	セッションの認証性	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28(1)	保存中の情報に対する保護 | 暗号化による保護	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28(3)	保存中の情報に対する保護 | 暗号化キー	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
SC-28(3)	保存中の情報に対する保護 | 暗号化キー	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。
SC-28	保存中の情報に対する保護	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	保存中の情報に対する保護	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
SC-28	保存中の情報に対する保護	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	保存中の情報に対する保護	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
SC-28	保存中の情報に対する保護	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	保存中の情報に対する保護	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	保存中の情報に対する保護	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	保存中の情報に対する保護	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	保存中の情報に対する保護	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	保存中の情報に対する保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
SC-28	保存中の情報に対する保護	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	保存中の情報に対する保護	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
SC-28	保存中の情報に対する保護	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
SC-28	保存中の情報に対する保護	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	保存中の情報に対する保護	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	保存中の情報に対する保護	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	保存中の情報に対する保護	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	保存中の情報に対する保護	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-28	保存中の情報に対する保護	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SC-28	保存中の情報に対する保護	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-36(2)	分散処理とストレージ | 同期	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
SC-36	分散処理とストレージ	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-36	分散処理とストレージ	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SC-36	分散処理とストレージ	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
SC-36	分散処理とストレージ	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2 (2)	欠陥修復 | 自動的な欠陥修復のステータス	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
SI-2 (2)	欠陥修復 | 自動的な欠陥修復のステータス	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2 (2)	欠陥修復 | 自動的な欠陥修復のステータス	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2(3)	欠陥の修復 | 欠陥の修復にかかる時間および修正アクションに関するベンチマーク	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2(3)	欠陥の修復 | 欠陥の修復にかかる時間および修正アクションに関するベンチマーク	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2(3)	欠陥の修復 | 欠陥の修復にかかる時間および修正アクションに関するベンチマーク	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
SI-2(4)	欠陥修復 | 自動パッチ管理ツール	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2(4)	欠陥修復 | 自動パッチ管理ツール	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2(4)	欠陥修復 | 自動パッチ管理ツール	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2(5)	欠陥修復 | ソフトウェアとファームウェアの自動更新	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
SI-2(5)	欠陥修復 | ソフトウェアとファームウェアの自動更新	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2(5)	欠陥修復 | ソフトウェアとファームウェアの自動更新	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
SI-2	欠陥修復	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
SI-2	欠陥修復	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-2	欠陥修復	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	s3-event-notifications-enabled	Amazon S3 イベント通知により、バケットオブジェクトに対する偶発的または意図的な変更について、関連する担当者に警告できます。アラートの例としては、新しいオブジェクトの作成、オブジェクトの削除、オブジェクトの復元、オブジェクトの紛失およびレプリケートなどが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-3(8)	悪意のあるコードからの保護 | 不正なコマンドの検知	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (1)	システムのモニタリング | システム全体の侵入検知システム	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (2)	システムモニタリング | リアルタイム分析のための自動化ツールとメカニズム	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
SI-4 (4)	システムのモニタリング | インバウンドとアウトバウンドの通信トラフィック	s3-event-notifications-enabled	Amazon S3 イベント通知により、バケットオブジェクトに対する偶発的または意図的な変更について、関連する担当者に警告できます。アラートの例としては、新しいオブジェクトの作成、オブジェクトの削除、オブジェクトの復元、オブジェクトの紛失およびレプリケートなどが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (4)	システムのモニタリング | インバウンドとアウトバウンドの通信トラフィック	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (5)	システムのモニタリング | システムで生成されたアラート	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4 (5)	システムのモニタリング | システムで生成されたアラート	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
SI-4 (5)	システムのモニタリング | システムで生成されたアラート	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(12)	システムモニタリング | 組織が生成する自動アラート	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(13)	システムモニタリング | トラフィックとイベントパターンの分析	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
SI-4(20)	システムモニタリング | 特権ユーザー	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(20)	システムモニタリング | 特権ユーザー	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(20)	システムモニタリング | 特権ユーザー	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
SI-4(20)	システムモニタリング | 特権ユーザー	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(20)	システムモニタリング | 特権ユーザー	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
SI-4(20)	システムモニタリング | 特権ユーザー	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(20)	システムモニタリング | 特権ユーザー	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(20)	システムモニタリング | 特権ユーザー	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(20)	システムモニタリング | 特権ユーザー	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(22)	システムモニタリング | 不正なネットワークサービス	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4(25)	システムモニタリング | ネットワークトラフィック分析の最適化	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
SI-4	システムモニタリング	s3-event-notifications-enabled	Amazon S3 イベント通知により、バケットオブジェクトに対する偶発的または意図的な変更について、関連する担当者に警告できます。アラートの例としては、新しいオブジェクトの作成、オブジェクトの削除、オブジェクトの復元、オブジェクトの紛失およびレプリケートなどが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	システムモニタリング	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-4	システムモニタリング	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7 (1)	ソフトウェア、ファームウェア、および情報の整合性 | 整合性の確認	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(3)	ソフトウェア、ファームウェア、および情報の整合性 | 一元管理された整合性ツール	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(6)	ソフトウェア、ファームウェア、および情報の整合性 | 暗号化による保護	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(7)	ソフトウェア、ファームウェア、および情報の整合性 | 検出と対応の統合	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-7(8)	ソフトウェア、ファームウェア、および情報の整合性 | 重要なイベントの監査機能	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の管理と保持	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の管理と保持	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の管理と保持	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の管理と保持	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の管理と保持	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の管理と保持	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-12	情報の管理と保持	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	s3-version-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-13(5)	予測可能な障害防止 | フェイルオーバー機能	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-20	汚染	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
SI-20	汚染	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
SI-20	汚染	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NIST 800-53 rev 5」で入手できます。

NIST 800 171 に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、NIST 800-171 と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の NIST 800-171 コントロールに関連付けられます。NIST の「800-171」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.1	システムへのアクセスを、権限のあるユーザー、権限のあるユーザーに代わって動作するプロセス、およびデバイス (他のシステムを含む) に制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.2	システムへのアクセスを、権限のあるユーザーが実行を許可されたトランザクションと機能のタイプに制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
3.1.3	承認された認可に従って CUI のフローをコントロールします。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.1.3	承認された認可に従って CUI のフローをコントロールします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
3.1.3	承認された認可に従って CUI のフローをコントロールします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.1.3	承認された認可に従って CUI のフローをコントロールします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
3.1.3	承認された認可に従って CUI のフローをコントロールします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.1.3	承認された認可に従って CUI のフローをコントロールします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3	承認された認可に従って CUI のフローをコントロールします。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.4	共謀をなくし、悪意のあるアクティビティのリスクを減らすために、個人の義務を分離します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.5	特定のセキュリティ機能や特権アカウントを含む、最小特権の原則を採用します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.6	セキュリティ以外の機能にアクセスする場合は、非特権アカウントまたはロールを使用します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
3.1.7	非特権ユーザーによる特権的機能の実行を防止し、それらの機能の実行を監査します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.7	非特権ユーザーによる特権的機能の実行を防止し、それらの機能の実行を監査します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.7	非特権ユーザーによる特権的機能の実行を防止し、それらの機能の実行を監査します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.7	非特権ユーザーによる特権的機能の実行を防止し、それらの機能の実行を監査します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.7	非特権ユーザーによる特権的機能の実行を防止し、それらの機能の実行を監査します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.7	非特権ユーザーによる特権的機能の実行を防止し、それらの機能の実行を監査します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.7	非特権ユーザーによる特権的機能の実行を防止し、それらの機能の実行を監査します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.12	リモートアクセスセッションをモニタリングおよびコントロールします。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.13	リモートアクセスセッションの機密性を保護するため、暗号化メカニズムを採用します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.14	管理されたアクセスコントロールポイントから、リモートアクセスをルーティングします。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.20	外部システムへの接続と使用を検証し、制御/制限します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1	違法、不正、または不適切なシステムアクティビティのモニタリング、分析、調査、報告を行うために必要な範囲で、システムの監査レコードを作成し、保持します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	個々のシステムユーザーのアクションで、それらのユーザーを一意に追跡することで、アクションに対する責任を負わせることができるようにします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.4	監査プロセスに障害が発生した場合に、アラートを生成します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.4	監査プロセスに障害が発生した場合に、アラートを生成します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.5	監査のレビュー、分析、報告プロセスを相関させて調査し、不適切、疑わしい、または異常なアクティビティの兆候に対応します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.5	監査のレビュー、分析、報告プロセスを相関させて調査し、不適切、疑わしい、または異常なアクティビティの兆候に対応します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
3.3.8	監査情報と監査ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.8	監査情報と監査ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.8	監査情報と監査ツールを、不正なアクセス、変更、削除から保護します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.8	監査情報と監査ツールを、不正なアクセス、変更、削除から保護します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.8	監査情報と監査ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
3.3.8	監査情報と監査ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.8	監査情報と監査ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.3.8	監査情報と監査ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.8	監査情報と監査ツールを、不正なアクセス、変更、削除から保護します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.1	各システムの開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、ドキュメントなど) のベースライン設定とインベントリを確立して維持します。	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.6	重要な機能のみを提供するように組織のシステムを設定することで、最小限の機能の原則を採用します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.4.7	不要な機能、ポート、プロトコル、またはサービスの使用を制限、無効化、および防止します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.7	不要な機能、ポート、プロトコル、またはサービスの使用を制限、無効化、および防止します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.7	不要な機能、ポート、プロトコル、またはサービスの使用を制限、無効化、および防止します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.7	不要な機能、ポート、プロトコル、またはサービスの使用を制限、無効化、および防止します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.9	ユーザーがインストールしたソフトウェアをコントロールおよびモニタリングします。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.9	ユーザーがインストールしたソフトウェアをコントロールおよびモニタリングします。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.2	組織のシステムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.2	組織のシステムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.2	組織のシステムへのアクセスを許可するための前提条件として、これらのユーザー、プロセス、またはデバイスの ID を認証 (または検証) します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.3	権限のあるアカウントへのローカルおよびネットワークアクセスと、権限のないアカウントへのネットワークアクセスに、多要素認証を使用します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.3	権限のあるアカウントへのローカルおよびネットワークアクセスと、権限のないアカウントへのネットワークアクセスに、多要素認証を使用します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.3	権限のあるアカウントへのローカルおよびネットワークアクセスと、権限のないアカウントへのネットワークアクセスに、多要素認証を使用します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.3	権限のあるアカウントへのローカルおよびネットワークアクセスと、権限のないアカウントへのネットワークアクセスに、多要素認証を使用します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.5	定義された期間の識別子の再利用を防止します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.6	定義されたアイドル状態の期間を経過したときに、識別子を無効にします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.7	新しいパスワードが作成される際、パスワードの複雑さと文字の変更を最小限に抑えます。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.8	指定した世代数でのパスワードの再利用を禁止します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.10	暗号で保護されたパスワードのみを保存および転送します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1	準備、検出、分析、抑制、回復、およびユーザーの応答アクティビティなど、組織のシステムで運用するインシデント処理機能を確立します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1	準備、検出、分析、抑制、回復、およびユーザーの応答アクティビティなど、組織のシステムで運用するインシデント処理機能を確立します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1	準備、検出、分析、抑制、回復、およびユーザーの応答アクティビティなど、組織のシステムで運用するインシデント処理機能を確立します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1	準備、検出、分析、抑制、回復、およびユーザーの応答アクティビティなど、組織のシステムで運用するインシデント処理機能を確立します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11.2	組織のシステムやアプリケーションの脆弱性を定期的にスキャンし、それらのシステムに影響を与える新たな脆弱性が発見された場合には、その脆弱性をスキャンします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11.2	組織のシステムやアプリケーションの脆弱性を定期的にスキャンし、それらのシステムに影響を与える新たな脆弱性が発見された場合には、その脆弱性をスキャンします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11.3	リスクの評価に従って脆弱性を修正します。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	api-gw-execution-logging-enabled	API Gateway の口グ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.1	情報システムの外部境界および主要な内部境界での通信 (組織のシステムによって送受信される情報など) をモニタリング、コントロールして保護します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効であることを確認することで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.2	組織のシステムにおいて効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技術、システムエンジニアリングの原則を採用します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.6	デフォルトでネットワーク通信トラフィックを拒否し、例外的にネットワーク通信トラフィックを許可します (すべてを拒否し、例外的に許可する)。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.6	デフォルトでネットワーク通信トラフィックを拒否し、例外的にネットワーク通信トラフィックを許可します (すべてを拒否し、例外的に許可する)。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.6	デフォルトでネットワーク通信トラフィックを拒否し、例外的にネットワーク通信トラフィックを許可します (すべてを拒否し、例外的に許可する)。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.8	物理的な代替の安全対策で保護されていない限り、送信中の CUI の不正な開示を防止するための暗号化メカニズムを実装します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.13.10	組織のシステムで採用されている暗号化で使用する暗号化キーを設定して管理します。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.10	組織のシステムで採用されている暗号化で使用する暗号化キーを設定して管理します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
3.13.16	保管中の CUI の機密性を確保します。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.16	保管中の CUI の機密性を確保します。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.13.16	保管中の CUI の機密性を確保します。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.16	保管中の CUI の機密性を確保します。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。
3.13.16	保管中の CUI の機密性を確保します。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.16	保管中の CUI の機密性を確保します。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
3.13.16	保管中の CUI の機密性を確保します。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.16	保管中の CUI の機密性を確保します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
3.13.16	保管中の CUI の機密性を確保します。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
3.13.16	保管中の CUI の機密性を確保します。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.16	保管中の CUI の機密性を確保します。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
3.13.16	保管中の CUI の機密性を確保します。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.16	保管中の CUI の機密性を確保します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
3.13.16	保管中の CUI の機密性を確保します。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.16	保管中の CUI の機密性を確保します。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.16	保管中の CUI の機密性を確保します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.16	保管中の CUI の機密性を確保します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
3.13.16	保管中の CUI の機密性を確保します。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.1	情報およびシステムの欠陥をタイムリーに特定、報告して修正します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.1	情報およびシステムの欠陥をタイムリーに特定、報告して修正します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.2	組織のシステム内の適切な場所で、悪意のあるコードから保護します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.2	組織のシステム内の適切な場所で、悪意のあるコードから保護します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.3	システムのセキュリティアラートとアドバイザリをモニタリングし、それに応じてアクションを実行します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.4	新しいリリースが利用可能になったら、悪意のあるコードからの保護メカニズムを更新します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6	攻撃や、潜在的な攻撃の兆候を検出するために、インバウンドおよびアウトバウンドの通信トラフィックを含む組織のシステムをモニタリングします。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
3.14.7	組織のシステムの不正使用を特定します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
3.14.7	組織のシステムの不正使用を特定します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
3.14.7	組織のシステムの不正使用を特定します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
3.14.7	組織のシステムの不正使用を特定します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7	組織のシステムの不正使用を特定します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NIST 800 171」で入手できます。

NIST の「800 172」の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、NIST 800-172 と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の NIST 800-172 コントロールに関連付けられます。NIST の「800-172」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	transfer solutions] を採用します。		
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	alb-desync-mode-check	HTTP Desync の脆弱性からアプリケーションを保護するには、アプリケーションロードバランサーで HTTP Desync 軽減モードが有効になっていることを確認してください。HTTP Desync の問題はリクエストスマグリングにつながり、アプリケーションがリクエストキューやキャッシュポイズニングに対して脆弱になる可能性があります。Desync 軽減モードの種類は、モニタリングモード、防御モード、厳密モードです。防御モードがデフォルトです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	clb-desync-mode-check	HTTP Desync の脆弱性からアプリケーションを保護するには、アプリケーションロードバランサーで HTTP Desync 軽減モードが有効になっていることを確認してください。HTTP Desync の問題はリクエストスマグリングにつながり、アプリケーションがリクエストキューやキャッシュポイズニングに対して脆弱になる可能性があります。Desync 軽減モードの種類は、モニタリングモード、防御モード、厳密モードです。防御モードがデフォルトです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	ec2-token-hop-limit-check	インスタンスメタデータサービス (IMDS) の HTTP PUT 応答が Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに限定されていることを確認します。IMDSv2 では、メタデータ応答ホップ制限が 1 (Config デフォルト) に設定されているため、シークレットトークンを含む PUT 応答は、インスタンスの外に移動することができません。この値が 1 より大きい場合、トークンは EC2 インスタンスから移動することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フローを制御するために、[Assignment: organization-defined secure information transfer solutions] を採用します。	nacl-no-unrestricted-ssh-rdp	ポート 22 (SSH) やポート 3389 (RDP) などのネットワークアクセスコントロールリスト (NACLs) のリモートサーバー管理ポートへのアクセスは、VPC 内のリソースへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
3.2.1e	ソーシャルエンジニアリング、高度持続的脅威行為者、侵入、不審な行動からの脅威の認識と対応に焦点を当てた意識向上トレーニング [Assignment: organization-defined frequency] を提供し、[Assignment: organization-defined frequency] または脅威に大きな変化があった場合にトレーニングを更新します。	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.2e	誤設定または未承認のシステムコンポーネントを検出するために自動化されたメカニズムを採用します。検出後、パッチ、再設定、またはその他の軽減措置を促進するために、[選択(一つまたは複数): コンポーネントを削除する、コンポーネントを検疫または修復ネットワークに配置する)] を実行します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
3.4.2e	誤設定または未承認のシステムコンポーネントを検出するために自動化されたメカニズムを採用します。検出後、パッチ、再設定、またはその他の軽減措置を促進するために、[選択(一つまたは複数): コンポーネントを削除する、コンポーネントを検疫または修復ネットワークに配置する)] を実行します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.2e	誤設定または未承認のシステムコンポーネントを検出するために自動化されたメカニズムを採用します。検出後、パッチ、再設定、またはその他の軽減措置を促進するために、[選択 (一つまたは複数): コンポーネントを削除する、コンポーネントを検疫または修復ネットワークに配置する)] を実行します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.2e	誤設定または未承認のシステムコンポーネントを検出するために自動化されたメカニズムを採用します。検出後、パッチ、再設定、またはその他の軽減措置を促進するために、[選択(一つまたは複数): コンポーネントを削除する、コンポーネントを検疫または修復ネットワークに配置する)] を実行します。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.3e	自動検出と管理ツールを使用し、システムコンポーネントの最新、完全、正確、かつ容易に入手可能なインベントリを維持します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.3e	自動検出と管理ツールを使用し、システムコンポーネントの最新、完全、正確、かつ容易に入手可能なインベントリを維持します。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
3.4.3e	自動検出と管理ツールを使用し、システムコンポーネントの最新、完全、正確、かつ容易に入手可能なインベントリを維持します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4.3e	自動検出と管理ツールを使用し、システムコンポーネントの最新、完全、正確、かつ容易に入手可能なインベントリを維持します。	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
3.4.3e	自動検出と管理ツールを使用し、システムコンポーネントの最新、完全、正確、かつ容易に入手可能なインベントリを維持します。	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.2e	多要素認証や複雑なアカウント管理には対応していないシステムおよびシステムコンポーネントのパスワードの生成、保護、ローテーション、管理のために自動化されたメカニズムを採用します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
3.5.2e	多要素認証や複雑なアカウント管理には対応していないシステムおよびシステムコンポーネントのパスワードの生成、保護、ローテーション、管理のために自動化されたメカニズムを採用します。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.2e	多要素認証や複雑なアカウント管理には対応していないシステムおよびシステムコンポーネントのパスワードの生成、保護、ローテーション、管理のために自動化されたメカニズムを採用します。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.2e	多要素認証や複雑なアカウント管理には対応していないシステムおよびシステムコンポーネントのパスワードの生成、保護、ローテーション、管理のために自動化されたメカニズムを採用します。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11.1e	リスク評価の一環として [Assignment: organization-defined sources of threat intelligence] を使用し、組織のシステム開発、セキュリティアーキテクチャ、セキュリティソリューションの選択、監視、脅威狩り、対応および復旧活動の指針とし、情報を提供することができます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.11.2e	サイバー脅威ハンティング活動 [選択 (1 つまたは複数): [Assignment: organization- defined frequency]、[Assignment: organization-defined event]] を実施して、[Assignment: organization-defined systems] の侵害指標を検索し、既存の管理を回避する脅威を検出、追跡、および破壊します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
3.11.5e	現在および蓄積された脅威情報に基づき、組織のシステムおよび組織に対する予想されるリスクに対処するためのセキュリティソリューション [Assignment: organization-defined frequency] の有効性を評価します。	annual-risk-assessment-performed (process check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	nacl-no-unrestricted-ssh-rdp	ポート 22 (SSH) やポート 3389 (RDP) などのネットワークアクセスコントロールリスト (NACLs) のリモートサーバー管理ポートへのアクセスは、VPC 内のリソースへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.13.4e	組織のシステムシステムと構成要素における [選択 (1 つまたは複数): [Assignment: organization-defined physical isolation techniques]、[Assignment: organization-defined logical isolation techniques]] を実行します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.1e	ルートオブトラスト機構または暗号署名を使用して、[Assignment: organization-defined security critical or essential software] の完全性を検証します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.2e	組織システムやシステムコンポーネントを継続的にモニタリングし、異常なアクティビティや疑わしいアクティビティがないことを確認します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
3.14.2e	組織システムやシステムコンポーネントを継続的にモニタリングし、異常なアクティビティや疑わしいアクティビティがないことを確認します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.2e	組織システムやシステムコンポーネントを継続的にモニタリングし、異常なアクティビティや疑わしいアクティビティがないことを確認します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.2e	組織システムやシステムコンポーネントを継続的にモニタリングし、異常なアクティビティや疑わしいアクティビティがないことを確認します。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.2e	組織システムやシステムコンポーネントを継続的にモニタリングし、異常なアクティビティや疑わしいアクティビティがないことを確認します。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.2e	組織システムやシステムコンポーネントを継続的にモニタリングし、異常なアクティビティや疑わしいアクティビティがないことを確認します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.2e	組織システムやシステムコンポーネントを継続的にモニタリングし、異常なアクティビティや疑わしいアクティビティがないことを確認します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.6e	[Assignment: organization-defined external organizations (割り当て: 組織で定義された外部組織)] から入手した脅威指標情報と効果的な緩和策を、侵入検知と脅威ハンティングの指針と情報に利用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7e	[Assignment: organization-defined security critical or essential software, firmware, and hardware components] の正しさを、[Assignment: organization-defined verification methods or techniques] を使って検証します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7e	[Assignment: organization-defined security critical or essential software, firmware, and hardware components] の正しさを、[Assignment: organization-defined verification methods or techniques] を使って検証します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7e	[Assignment: organization-defined security critical or essential software, firmware, and hardware components] の正しさを、[Assignment: organization-defined verification methods or techniques] を使って検証します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7e	[Assignment: organization-defined security critical or essential software, firmware, and hardware components] の正しさを、[Assignment: organization-defined verification methods or techniques] を使って検証します。	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。 AWS Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 はプラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.14.7e	[Assignment: organization-defined security critical or essential software, firmware, and hardware components] の正しさを、[Assignment: organization-defined verification methods or techniques] を使って検証します。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NIST 800 172」で入手できます。

NIST の「800 181」の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、NIST 800 181 と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の NIST 800 181 コントロールに関連付けられます。NIST の「800-181」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0008	データ容量要件の予測される変化を分析し、計画します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。
T0008	データ容量要件の予測される変化を分析し、計画します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサー

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ビスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
T0008	データ容量要件の予測される変化を分析し、計画します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0008	データ容量要件の予測される変化を分析し、計画します。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
T0008	データ容量要件の予測される変化を分析し、計画します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0008	データ容量要件の予測される変化を分析し、計画します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0008	データ容量要件の予測される変化を分析し、計画します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0008	データ容量要件の予測される変化を分析し、計画します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0008	データ容量要件の予測される変化を分析し、計画します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0008	データ容量要件の予測される変化を分析し、計画します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
T0008	データ容量要件の予測される変化を分析し、計画します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0008	データ容量要件の予測される変化を分析し、計画します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0008	データ容量要件の予測される変化を分析し、計画します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
T0008	データ容量要件の予測される変化を分析し、計画します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elasticsearch Service (Amazon ES) ドメインで暗号化が有効になっていることを確認します。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0017	サービス指向のセキュリティアーキテクチャの原則を適用し、組織の機密性、完全性、可用性の要件を満たすことができます。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0024	システムのサイバーセキュリティ報告書を満たすために必要なデータを収集し、維持します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
T0042	サイバーディフェンスアナリストと調整し、特殊なサイバーディフェンスアプリケーションのルールとシグネチャ (侵入検知/保護システム、アンチウイルス、コンテンツブラックリストなど) の更新を管理し運営します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0047	インシデントデータを関連付け、特定の脆弱性を特定し、迅速な改善を可能にするための提案を行います。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、システム要件が適切な災害復旧と運用継続の要件を特定することを確実にします。これには、適切なフェイルオーバー/代替サイト要件、バックアップ要件、システム復旧/復元に関する材料支持性要件が含まれます。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0065	ネットワークのバックアップとリカバリーの手順を開発し、実施します。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0070	開発中のシステムのディザスターリカバリーおよびオペレーション継続計画を策定し、システムが本番環境に入る前に確実にテストする。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0086	システム設計に組み込まれた商用製品のセキュリティパッチのアプリケーションが、意図された動作環境の管理当局によって指示されたタイムラインを満たすことを保証します。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
T0086	システム設計に組み込まれた商用製品のセキュリティパッチのアプリケーションが、意図された動作環境の管理当局によって指示されたタイムラインを満たすことを保証します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0086	システム設計に組み込まれた商用製品のセキュリティパッチのアプリケーションが、意図された動作環境の管理当局によって指示されたタイムラインを満たすことを保証します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0086	システム設計に組み込まれた商用製品のセキュリティパッチのアプリケーションが、意図された動作環境の管理当局によって指示されたタイムラインを満たすことを保証します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0110	セキュリティインシデントが、特定の法的措置を必要とする法律違反を示唆するものであるかどうかを特定および/または判断する。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0110	セキュリティインシデントが、特定の法的措置を必要とする法律違反を示唆するものであるかどうかを特定および/または判断する。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0110	セキュリティインシデントが、特定の法的措置を必要とする法律違反を示唆するものであるかどうかを特定および/または判断する。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
T0128	システムソフトウェアのアップデートやパッチの自動化機能を実用的な範囲で統合し、システムの運用環境における現在および予測されるパッチのタイムライン要件に基づいて、システムソフトウェアの手動アップデートやパッチのプロセスと手順を開発します。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0128	システムソフトウェアのアップデートやパッチの自動化機能を実用的な範囲で統合し、システムの運用環境における現在および予測されるパッチのタイムライン要件に基づいて、システムソフトウェアの手動アップデートやパッチのプロセスと手順を開発します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
T0128	システムソフトウェアのアップデートやパッチの自動化機能を実用的な範囲で統合し、システムの運用環境における現在および予測されるパッチのタイムライン要件に基づいて、システムソフトウェアの手動アップデートやパッチのプロセスと手順を開発します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0128	システムソフトウェアのアップデートやパッチの自動化機能を実用的な範囲で統合し、システムの運用環境における現在および予測されるパッチのタイムライン要件に基づいて、システムソフトウェアの手動アップデートやパッチのプロセスと手順を開発します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	opensearch-in-vpc-only	Amazon Elasticsearch Service (Amazon ES) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon ES ドメインを Amazon VPC に配置すると、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用せずに、Amazon ES と Amazon VPC 内の他のサービス間の安全な通信が実現できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0144	管理アカウント、ネットワーク権限、システムや装置へのアクセス。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0151	エンタープライズが計画した保護レベルを提供しているかを確認するため、サイバーセキュリティセイフガードの有効性をモニタリングして評価します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0151	エンタープライズが計画した保護レベルを提供しているかを確認するため、サイバーセキュリティセイフガードの有効性をモニタリングして評価します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0151	エンタープライズが計画した保護レベルを提供しているかを確認するため、サイバーセキュリティセイフガードの有効性をモニタリングして評価します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0152	最適パフォーマンスを確保するため、データベースをモニタリングしてメンテナンスします。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0153	ネットワークの容量とパフォーマンスを監視します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0153	ネットワークの容量とパフォーマンスを監視します。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
T0153	ネットワークの容量とパフォーマンスを監視します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0153	ネットワークの容量とパフォーマンスを監視します。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0154	知識管理アセットとリソースの使用をモニタリングして報告します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
T0156	設定管理に関して監視し、推薦します。	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0156	設定管理に関して監視し、推薦します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0156	設定管理に関して監視し、推薦します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0156	設定管理に関して監視し、推薦します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0156	設定管理に関して監視し、推薦します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0156	設定管理に関して監視し、推薦します。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0156	設定管理に関して監視し、推薦します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0156	設定管理に関して監視し、推薦します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0156	設定管理に関して監視し、推薦します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0160	情報が外部の第3者から保護されていることを確保するため、ネットワークの脆弱性をパッチします。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0160	情報が外部の第3者から保護されていることを確保するため、ネットワークの脆弱性をパッチします。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0160	情報が外部の第3者から保護されていることを確保するため、ネットワークの脆弱性をパッチします。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0162	データの整合性を確保するためデータベースのバックアップとリカバリを行います。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0166	状況認識をして、実際の攻撃の有効性を究明するため、エンタープライズ内で様々な出展から集めた情報を使ってイベント相関を行います。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0168	確立されたデータベースとハッシュ比較を行います。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	opensearch-in-vpc-only	Amazon Elasticsearch Service (Amazon ES) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon ES ドメインを Amazon VPC に配置すると、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用せずに、Amazon ES と Amazon VPC 内の他のサービス間の安全な通信が実現できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0195	ミッション要求に基づいて、(ウェブベースポータルなどを経由して)関連情報のマネージドフローを提供します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0215	セキュリティ違反の可能性を認識し、必要に応じて適切な行動をとり、報告します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0244	アプリケーションソフトウェア、ネットワーク、システムセキュリティの配置を前述のとおり行うことを確認し、偏向を記録し、変更を訂正する要求されたアクションを寸証します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0244	アプリケーションソフトウェア、ネットワーク、システムセキュリティの配置を前述のとおり行うことを確認し、偏向を記録し、変更を訂正する要求されたアクションを寸証します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0244	アプリケーションソフトウェア、ネットワーク、システムセキュリティの配置を前述のとおり行うことを確認し、偏向を記録し、変更を訂正する要求されたアクションを寸証します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0258	適時の検出、識別、起こり得る攻撃、侵入、異常・誤用のアクティビティに対するアラートにより、これらのインシデントやイベントを無害なアクティビティと区別します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0259	悪意のあるアクティビティを識別するため、継続的なモニタリングとシステムアクティビティを分析するサイバー防衛ツールを使用します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	opensearch-in-vpc-only	Amazon Elasticsearch Service (Amazon ES) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon ES ドメインを Amazon VPC に配置すると、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用せずに、Amazon ES と Amazon VPC 内の他のサービス間の安全な通信が実現できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0262	承認済みの鉄壁の防衛プリンシパルとプラクティスを実行します。(例: 多様な場所の防衛、多層防衛、セキュリティの堅牢性)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、 AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	opensearch-in-vpc-only	Amazon Elasticsearch Service (Amazon ES) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon ES ドメインを Amazon VPC に配置すると、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用せずに、Amazon ES と Amazon VPC 内の他のサービス間の安全な通信が実現できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0284	サイバーセキュリティ関連の新規ツールや技術を設計・開発します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0306	インシデント管理、サービスレベル管理、変更管理、リリース管理、継続管理、データベースやデータ管理システムの利用管理を支援します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0306	インシデント管理、サービスレベル管理、変更管理、リリース管理、継続管理、データベースやデータ管理システムの利用管理を支援します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0306	インシデント管理、サービスレベル管理、変更管理、リリース管理、継続管理、データベースやデータ管理システムの利用管理を支援します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0314	システムセキュリティのコンテクスト、予備のシステムセキュリティ Concept of Operations (CONOPS) を開発し、該当するサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0314	システムセキュリティのコンテクスト、予備のシステムセキュリティ Concept of Operations (CONOPS) を開発し、該当するサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義します。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
T0314	システムセキュリティのコンテクスト、予備のシステムセキュリティ Concept of Operations (CONOPS) を開発し、該当するサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義します。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0314	システムセキュリティのコンテクスト、予備のシステムセキュリティ Concept of Operations (CONOPS) を開発し、該当するサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義します。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
T0314	システムセキュリティのコンテクスト、予備のシステムセキュリティ Concept of Operations (CONOPS) を開発し、該当するサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義します。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0314	システムセキュリティのコンテクスト、予備のシステムセキュリティ Concept of Operations (CONOPS) を開発し、該当するサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0333	サイバー防衛傾向分析と報告を行います。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0333	サイバー防衛傾向分析と報告を行います。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0347	出典データと後続の結果検証へアクセスします。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0358	特権的アクセスユーザーのためのシステム管理と管理機能を設計し開発します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
T0358	特権的アクセスユーザーのためのシステム管理と管理機能を設計し開発します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0358	特権的アクセスユーザーのためのシステム管理と管理機能を設計し開発します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0358	特権的アクセスユーザーのためのシステム管理と管理機能を設計し開発します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0358	特権的アクセスユーザーのためのシステム管理と管理機能を設計し開発します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0358	特権的アクセスユーザーのためのシステム管理と管理機能を設計し開発します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0358	特権的アクセスユーザーのためのシステム管理と管理機能を設計し開発します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
T0358	特権的アクセスユーザーのためのシステム管理と管理機能を設計し開発します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0376	組織の要件に従って、サイバー従業員管理プログラムを構築、調達、実施、アクセスします。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
T0416	既設の public key infrastructure (PKI) ライブラリーを利用し、適切な場合証明書管理と暗号化機能を統合することでパブリックキーを有効にします。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0421	インデックス作成、カタログ作成、ストレージ、系統だった組織の知識へのアクセスを管理します。(例: ハードコピーの文書、デジタルファイル)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	opensearch-in-vpc-only	Amazon Elasticsearch Service (Amazon ES) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon ES ドメインを Amazon VPC に配置すると、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用せずに、Amazon ES と Amazon VPC 内の他のサービス間の安全な通信が実現できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0475	最小特権と必要最小限のプリンシパルに基づいて十分なアクセス制御にアクセスします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0489	機密保持、インテグリティ、可用性、認証、否認防止を確保するため確率した手続きに基づいて、システムセキュリティの方策を実行します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0491	組織のスタンダードに基づいて、システムユーザー用のハードウェア、ソフトウェア、周辺機器をインストールし、設定する。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0491	組織のスタンダードに基づいて、システムユーザー用のハードウェア、ソフトウェア、周辺機器をインストールし、設定する。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0491	組織のスタンダードに基づいて、システムユーザー用のハードウェア、ソフトウェア、周辺機器をインストールし、設定する。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
T0503	サイバー防衛脅威状況の最新性を保持し、セキュリティ問題がエンタープライズに影響を与える可能性のあるのか断定することで、外部データの出典をモニタリングします。(例: サイバー防衛ベンダーサイト、コンピュータ緊急対応チーム、セキュリティフォーカス)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0509	情報セキュリティリスク評価を実行します。	annual-risk-assessment-performed (process check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	elasticsearch-node-to-node-encryption-check	Amazon Elasticsearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	opensearch-encrypt ed-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elasticsearch Service (Amazon ES) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	opensearch-node-to-node-encryption-check	Amazon Elasticsearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elasticsearch Service (Amazon ES) ドメインで暗号化が有効になっていることを確認します。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0553	悪用機会を減らすため、サイバーセキュリティ機能を適用します (例: 暗号化、アクセス制御、アイデンティティ管理)。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
T0557	サイバー空間関連のキー管理機能を統合します。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達したときにキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0557	サイバー空間関連のキー管理機能を統合します。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0576	全出典の機密情報にアクセスし、サイバーオペレーションの目的を支援するためターゲットを推薦します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	elasticsearch-in-vpc-only	Amazon Elasticsearch Service (Amazon ES) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon ES ドメインを Amazon VPC に配置すると、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用せずに、Amazon ES と Amazon VPC 内の他のサービス間の安全な通信が実現できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	opensearch-in-vpc-only	Amazon Elasticsearch Service (Amazon ES) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon ES ドメインを Amazon VPC に配置すると、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用せずに、Amazon ES と Amazon VPC 内の他のサービス間の安全な通信が実現できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0609	ワイヤレスコンピュータとデジタルネットワークへのアクセスができるようにします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0616	ネットワーク内のシステムのネットワークスカウティングと脆弱性分析を実施します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
T0686	脅威の脆弱性を識別します。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0686	脅威の脆弱性を識別します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	elasticsearch-logs-to-cloudwatch	Amazon Elasticsearch service ドメインでエラーログが有効になっていて、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0706	従来の技術や代替技術を用いたネットワークに関する情報を就職活動します (例: ソーシャルネットワーク分析、連鎖法の要求、トラフィック分析)。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0777	ネットワーク、システム管理者、アクティビティを書きます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0805	インテリジェンスに基づく重要なネットワークイベントや侵入を報告します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0877	消費者情報のアクセス権を監督するために、該当する組織部門と協力します	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7
T0935	情報セキュリティリスク評価を実行します。	annual-risk-assessment-performed (process check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0960	システムおよびその動作環境の変化を監視する。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。
T0960	システムおよびその動作環境の変化を監視する。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0960	システムおよびその動作環境の変化を監視する。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0960	システムおよびその動作環境の変化を監視する。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0960	システムおよびその動作環境の変化を監視する。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0960	システムおよびその動作環境の変化を監視する。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0960	システムおよびその動作環境の変化を監視する。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
T0960	システムおよびその動作環境の変化を監視する。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0992	継続的なモニタリングの結果を継続的な認可にどのように使用するかを決定します。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager シークレットのローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
T0993	継続的な監視ツールや技術アクセス制御のプロセスや手順を確立します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NIST 800 181」で入手できます。

NIST の「1800 25」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、NIST 1800-25 と AWS マネージド Config ルール間のマッピングの例を示します。各 は特定の AWS リソース AWS Config に適用され、1 つ以上の NIST 1800-25 コントロールに関連付けら

れます。NIST 1800-25 コントロールは、複数の AWS Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ち

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-1	アセットの脆弱性が特定され、ドキュメント化されている	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
ID.RA-1	アセットの脆弱性が特定され、ドキュメント化されている	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-1	アセットの脆弱性が特定され、ドキュメント化されている	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-1	アセットの脆弱性が特定され、ドキュメント化されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
PR.AC-3	リモートアクセスが管理されている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
PR.AC-3	リモートアクセスが管理されている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-3	リモートアクセスが管理されている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
PR.AC-3	リモートアクセスが管理されている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-3	リモートアクセスが管理されている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
PR.AC-3	リモートアクセスが管理されている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.AC-3	リモートアクセスが管理されている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
PR.DS-1	保管中のデータが保護されている	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
PR.DS-1	保管中のデータが保護されている	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
PR.DS-1	保管中のデータが保護されている	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
PR.DS-1	保管中のデータが保護されている	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
PR.DS-2	転送中のデータが保護されている	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
PR.DS-2	転送中のデータが保護されている	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
PR.DS-2	転送中のデータが保護されている	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
PR.DS-2	転送中のデータが保護されている	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-6	整合性チェックのメカニズムが、ソフトウェア、ファームウェア、および情報の整合性を検証するために使用されている	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-6	整合性チェックのメカニズムが、ソフトウェア、ファームウェア、および情報の整合性を検証するために使用されている	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-3	設定の変更管理プロセスが実施されている	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
PR.IP-3	設定の変更管理プロセスが実施されている	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-9	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	response-plan-exists-maintained (Process Check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。正式にドキュメント化された更新済みの対応計画を用意することで、対応する担当者がインシデントの発生中に従うべき役割、責任、プロセスを理解することができます。
PR.IP-10	インシデント対応および復旧計画がテストされている	response-plan-tested (Process Check)	インシデント対応と復旧計画がテスト済みであることを確認します。これにより、インシデント発生時に計画が有効であるか、ギャップや更新に対処する必要があるかどうかを理解することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-12	脆弱性の管理計画が作成され、実装されている	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。これには、脆弱性管理ツール、環境スキャンの周期、役割と責任などが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-12	脆弱性の管理計画が作成され、実装されている	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-12	脆弱性の管理計画が作成され、実装されている	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-12	脆弱性の管理計画が作成され、実装されている	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.MA-2	組織のアセットのリモートメンテナンスが承認され、記録され、不正アクセスを防止する方法で実行されている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.MA-2	組織のアセットのリモートメンテナンスが承認され、記録され、不正アクセスを防止する方法で実行されている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセスの監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	通信およびコントロールネットワークが保護されている	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
PR.PT-4	通信およびコントロールネットワークが保護されている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS Foundational Security Best Practices 値: 90)。実際の値には、組織のポリシーを反映する必要があります。
PR.PT-4	通信およびコントロールネットワークが保護されている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-4	通信およびコントロールネットワークが保護されている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
PR.PT-4	通信およびコントロールネットワークが保護されている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-4	通信およびコントロールネットワークが保護されている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.PT-4	通信およびコントロールネットワークが保護されている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループ上のすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-8	脆弱性スキャンが実行されている	vuln-scans-performed (Process Check)	コンプライアンス要件に従って脆弱性スキャンが実行されていることを確認します。スキャンの周期、使用するツール、結果の使用方法については、組織が定義する必要があります。
RS.MI-3	新たに特定された脆弱性が修正されるか、受け入れられたリスクとしてドキュメント化されている	vuln-mitigated-accepted (Process Check)	新たに特定された脆弱性が修正されるか、受け入れられたリスクとしてドキュメント化されるようにします。 AWS Security Hub、Amazon Guard Duty、Amazon Inspector、Config AWS などのサービスは、環境内の脆弱性の特定に役立ちます。組織のコンプライアンス要件に従って、脆弱性を修正するか、リスクとして承諾する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.MI-3	新たに特定された脆弱性が修正されるか、受け入れられたリスクとしてドキュメント化されている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NIST 1800 25」で入手できます。

NIST の「CSF」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するよう

には設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、NIST Cyber Security Framework (CSF) と AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の NIST CSF コントロールに関連付けられます。NIST の「CSF」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できま

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			す。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-1	ユーザーとシステムのネットワークオペレーションと、予測されるデータフローのベースラインが確立され、管理されている	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-2	検出されたイベントが、攻撃のターゲットと方法を理解するために分析されている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-2	検出されたイベントが、攻撃のターゲットと方法を理解するために分析されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-3	イベントデータが、複数のソースとセンサーから収集され、関連付けられている	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
DE.AE-4	イベントの影響が判断されている	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-4	イベントの影響が判断されている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-4	イベントの影響が判断されている	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-4	イベントの影響が判断されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-4	イベントの影響が判断されている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-4	イベントの影響が判断されている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-4	イベントの影響が判断されている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.AE-4	イベントの影響が判断されている	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	s3-event-notifications-enabled	Amazon S3 イベント通知により、バケットオブジェクトに対する偶発的または意図的な変更について、関連する担当者に警告できます。アラートの例としては、新しいオブジェクトの作成、オブジェクトの削除、オブジェクトの復元、オブジェクトの紛失およびレプリケートなどが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-1	潜在的なサイバーセキュリティイベントを検出するため、ネットワークがモニタリングされている	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
DE.CM-3	潜在的なサイバーセキュリティイベントを検出するため、担当者のアクティビティがモニタリングされている	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-3	潜在的なサイバーセキュリティイベントを検出するため、担当者のアクティビティがモニタリングされている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-3	潜在的なサイバーセキュリティイベントを検出するため、担当者のアクティビティがモニタリングされている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-3	潜在的なサイバーセキュリティイベントを検出するため、担当者のアクティビティがモニタリングされている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-3	潜在的なサイバーセキュリティイベントを検出するため、担当者のアクティビティがモニタリングされている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-3	潜在的なサイバーセキュリティイベントを検出するため、担当者のアクティビティがモニタリングされている	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-4	悪意のあるコードが検出されている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-4	悪意のあるコードが検出されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-5	不正なモバイルコードが検出されている	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
DE.CM-5	不正なモバイルコードが検出されている	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-5	不正なモバイルコードが検出されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-5	不正なモバイルコードが検出されている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-5	不正なモバイルコードが検出されている	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-5	不正なモバイルコードが検出されている	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-6	潜在的なサイバーセキュリティイベントを検出するため、外部のサービスプロバイダーのアクティビティがモニタリングされている	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
DE.CM-6	潜在的なサイバーセキュリティイベントを検出するため、外部のサービスプロバイダーのアクティビティがモニタリングされている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-6	潜在的なサイバーセキュリティイベントを検出するため、外部のサービスプロバイダーのアクティビティがモニタリングされている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-6	潜在的なサイバーセキュリティイベントを検出するため、外部のサービスプロバイダーのアクティビティがモニタリングされている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-6	潜在的なサイバーセキュリティイベントを検出するため、外部のサービスプロバイダーのアクティビティがモニタリングされている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-6	潜在的なサイバーセキュリティイベントを検出するため、外部のサービスプロバイダーのアクティビティがモニタリングされている	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが実行されている	api-gw-execution-logging-enabled	API Gateway の口グ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが実行されている	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが実行されている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが実行されている	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが実行されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが実行されている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが実行されている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが実行されている	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが実行されている	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.DP-4	イベント検出情報が伝達されている	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
DE.DP-4	イベント検出情報が伝達されている	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.DP-4	イベント検出情報が伝達されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.DP-4	イベント検出情報が伝達されている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.DP-4	イベント検出情報が伝達されている	s3-event-notifications-enabled	Amazon S3 イベント通知により、バケットオブジェクトに対する偶発的または意図的な変更について、関連する担当者に警告できます。アラートの例としては、新しいオブジェクトの作成、オブジェクトの削除、オブジェクトの復元、オブジェクトの紛失およびレプリケートなどが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.DP-4	イベント検出情報が伝達されている	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.DP-4	イベント検出情報が伝達されている	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
DE.DP-5	検出プロセスが継続的に改善されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。
ID.AM-2	組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-3	組織の通信とデータフローがマッピングされている	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
ID.AM-3	組織の通信とデータフローがマッピングされている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-3	組織の通信とデータフローがマッピングされている	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-3	組織の通信とデータフローがマッピングされている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-3	組織の通信とデータフローがマッピングされている	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-3	組織の通信とデータフローがマッピングされている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.AM-3	組織の通信とデータフローがマッピングされている	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.BE-5	重要なサービスの提供をサポートするための回復性の要件が、すべての運用状況に対して確立されている (例: 強迫/攻撃中、復旧中、通常の運用中)	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-1	アセットの脆弱性が特定され、ドキュメント化されている	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。
ID.RA-1	アセットの脆弱性が特定され、ドキュメント化されている	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-1	アセットの脆弱性が特定され、ドキュメント化されている	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-1	アセットの脆弱性が特定され、ドキュメント化されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-2	サイバー脅威インテリジェンスを情報共有フォーラムやソースから受信しいる	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
ID.RA-3	内部および外部の両方の脅威が特定され、ドキュメント化されている	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-3	内部および外部の両方の脅威が特定され、ドキュメント化されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
ID.RA-5	脅威、脆弱性、可能性、および影響を、リスクを判断するために使用する	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-5	脅威、脆弱性、可能性、および影響を、リスクを判断するために使用する	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-5	脅威、脆弱性、可能性、および影響を、リスクを判断するために使用する	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.RA-5	脅威、脆弱性、可能性、および影響を、リスクを判断するために使用する	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.SC-4	サプライヤーと第三者パートナーは、監査、テスト結果、またはその他の形式の評価を使用して定期的に評価され、契約上の義務を果たしていることを確認します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
ID.SC-4	サプライヤーと第三者パートナーは、監査、テスト結果、またはその他の形式の評価を使用して定期的に評価され、契約上の義務を果たしていることを確認します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.SC-4	サプライヤーと第三者パートナーは、監査、テスト結果、またはその他の形式の評価を使用して定期的に評価され、契約上の義務を果たしていることを確認します。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.SC-4	サプライヤーと第三者パートナーは、監査、テスト結果、またはその他の形式の評価を使用して定期的に評価され、契約上の義務を果たしていることを確認します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager シークレットのローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-1	ID と認証情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、監査されている	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
PR.AC-3	リモートアクセスが管理されている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
PR.AC-3	リモートアクセスが管理されている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-3	リモートアクセスが管理されている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
PR.AC-3	リモートアクセスが管理されている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-3	リモートアクセスが管理されている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.AC-3	リモートアクセスが管理されている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-3	リモートアクセスが管理されている	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-6	ID が証明され、認証情報にバインドされ、やり取り中にアサートされている	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-6	ID が証明され、認証情報にバインドされ、やり取り中にアサートされている	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-7	ユーザー、デバイス、およびその他のアセットが、トランザクションのリスク (例: 個人のセキュリティおよびプライバシーのリスクやその他の組織のリスク) に応じて認証されている (例: 単一要素認証、多要素認証)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基本的なセキュリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
PR.AC-7	ユーザー、デバイス、およびその他のアセットが、トランザクションのリスク (例: 個人のセキュリティおよびプライバシーのリスクやその他の組織のリスク) に応じて認証されている (例: 単一要素認証、多要素認証)	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-7	ユーザー、デバイス、およびその他のアセットが、トランザクションのリスク (例: 個人のセキュリティおよびプライバシーのリスクやその他の組織のリスク) に応じて認証されている (例: 単一要素認証、多要素認証)	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-7	ユーザー、デバイス、およびその他のアセットが、トランザクションのリスク (例: 個人のセキュリティおよびプライバシーのリスクやその他の組織のリスク) に応じて認証されている (例: 単一要素認証、多要素認証)	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-7	ユーザー、デバイス、およびその他のアセットが、トランザクションのリスク (例: 個人のセキュリティおよびプライバシーのリスクやその他の組織のリスク) に応じて認証されている (例: 単一要素認証、多要素認証)	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
PR.AT-1	ユーザー全員への周知とトレーニングの実施	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで Key Management Service (AWS KMS) を使用した AWS 暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
PR.DS-1	保管中のデータが保護されている	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
PR.DS-1	保管中のデータが保護されている	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
PR.DS-1	保管中のデータが保護されている	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
PR.DS-1	保管中のデータが保護されている	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-1	保管中のデータが保護されている	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-1	保管中のデータが保護されている	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで Key Management Service (AWS KMS) による AWS 暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
PR.DS-2	転送中のデータが保護されている	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
PR.DS-2	転送中のデータが保護されている	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
PR.DS-2	転送中のデータが保護されている	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
PR.DS-2	転送中のデータが保護されている	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-2	転送中のデータが保護されている	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-3	アセットが、削除、転送、廃棄のすべてにおいて正式に管理されている	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-3	アセットが、削除、転送、廃棄のすべてにおいて正式に管理されている	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-3	アセットが、削除、転送、廃棄のすべてにおいて正式に管理されている	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
PR.DS-4	十分な容量で可用性が維持されている	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
PR.DS-4	十分な容量で可用性が維持されている	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
PR.DS-4	十分な容量で可用性が維持されている	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-4	十分な容量で可用性が維持されている	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
PR.DS-5	データ漏洩に対する保護が実装されている	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、 AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。
PR.DS-5	データ漏洩に対する保護が実装されている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
PR.DS-5	データ漏洩に対する保護が実装されている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.DS-5	データ漏洩に対する保護が実装されている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.DS-5	データ漏洩に対する保護が実装されている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-5	データ漏洩に対する保護が実装されている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
PR.DS-5	データ漏洩に対する保護が実装されている	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-6	整合性チェックのメカニズムが、ソフトウェア、ファームウェア、および情報の整合性を検証するために使用されている	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-6	整合性チェックのメカニズムが、ソフトウェア、ファームウェア、および情報の整合性を検証するために使用されている	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-7	開発環境とテスト環境が本番環境と分離されている	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-7	開発環境とテスト環境が本番環境と分離されている	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
PR.DS-7	開発環境とテスト環境が本番環境と分離されている	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-7	開発環境とテスト環境が本番環境と分離されている	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
PR.DS-7	開発環境とテスト環境が本番環境と分離されている	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-7	開発環境とテスト環境が本番環境と分離されている	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	account-part-of-organizations	Organizations AWS アカウント 内の AWS の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成します。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-1	情報テクノロジー/産業用コントロールシステムのベースライン設定は、セキュリティの原則 (最小限の機能の概念など) を組み込んで作成および維持されている	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-2	システムを管理するシステム開発ライフサイクルが実装されている	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-2	システムを管理するシステム開発ライフサイクルが実装されている	codebuild-project-source-repo-url-check	GitHub または Bitbucket のソースレポジトリの URL に、 AWS Codebuild プロジェクト環境内の個人用のアクセストークン、サインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-2	システムを管理するシステム開発ライフサイクルが実装されている	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-3	設定の変更管理プロセスが実施されている	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
PR.IP-3	設定の変更管理プロセスが実施されている	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-4	情報のバックアップが実施、維持、テストされている	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-7	保護プロセスが改善されている	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
PR.IP-8	保護技術の有効性が共有されている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-8	保護技術の有効性が共有されている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.IP-8	保護技術の有効性が共有されている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-8	保護技術の有効性が共有されている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
PR.IP-8	保護技術の有効性が共有されている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-8	保護技術の有効性が共有されている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-8	保護技術の有効性が共有されている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.IP-8	保護技術の有効性が共有されている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-8	保護技術の有効性が共有されている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.IP-8	保護技術の有効性が共有されている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-8	保護技術の有効性が共有されている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-8	保護技術の有効性が共有されている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-12	脆弱性の管理計画が作成され、実装されている	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-12	脆弱性の管理計画が作成され、実装されている	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリに役立ちます。 AWS Systems Manager では、マネージドインスタンスに設定のステータスを割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.IP-12	脆弱性の管理計画が作成され、実装されている	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.MA-2	組織のアセットのリモートメンテナンスが承認され、記録され、不正アクセスを防止する方法で実行されている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.MA-2	組織のアセットのリモートメンテナンスが承認され、記録され、不正アクセスを防止する方法で実行されている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセスの監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	通信およびコントロールネットワークが保護されている	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACL で AWS WAF (V2) ログ記録を有効にします。 ACLs AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウントの情報、IP アドレス、イベント発生時刻が含まれます。
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-1	監査およびログレコードが、ポリシーに従って決定、ドキュメント化、実装、レビューされている	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
PR.PT-4	通信およびコントロールネットワークが保護されている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
PR.PT-4	通信およびコントロールネットワークが保護されている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-4	通信およびコントロールネットワークが保護されている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
PR.PT-4	通信およびコントロールネットワークが保護されている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-4	通信およびコントロールネットワークが保護されている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.PT-4	通信およびコントロールネットワークが保護されている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-4	通信およびコントロールネットワークが保護されている	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-5	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RC.RP-1	サイバーセキュリティインシデント発生時、または発生後にリカバリープランを実行します	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.AN-2	インシデントの影響が把握されている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.MI-3	新たに特定された脆弱性が修正されるか、受け入れられたリスクとしてドキュメント化されている	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、バックアッププランが最小頻度と保持期間に設定されていることを確認します AWS 。AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の値には、組織の要件を反映する必要があります。
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが Backup プランの一部 AWS であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
RS.RP-1	インシデント発生中または発生後に対応計画が実施される	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NIST CSF」で入手できます。

NIST プライバシーフレームワーク v1.0 オペレーションのベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成

できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、NIST の「Privacy Framework」と、 AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の NIST プライバシーフレームワークコントロールに関連付けられます。NIST プライバシーフレームワークコントロールは、複数の AWS Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P7	処理許可と関連するデータ値をデータ要素とともに送信するメカニズムが確立され、実施されています。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CT.DM-P7	処理許可と関連するデータ値をデータ要素とともに送信するメカニズムが確立され、実施されています。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P7	処理許可と関連するデータ値をデータ要素とともに送信するメカニズムが確立され、実施されています。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CT.DM-P7	処理許可と関連するデータ値をデータ要素とともに送信するメカニズムが確立され、実施されています。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P7	処理許可と関連するデータ値をデータ要素とともに送信するメカニズムが確立され、実施されています。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
CT.DM-P7	処理許可と関連するデータ値をデータ要素とともに送信するメカニズムが確立され、実施されています。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P7	処理許可と関連するデータ値をデータ要素とともに送信するメカニズムが確立され、実施されています。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CT.DM-P7	処理許可と関連するデータ値をデータ要素とともに送信するメカニズムが確立され、実施されています。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P7	処理許可と関連するデータ値をデータ要素とともに送信するメカニズムが確立され、実施されています。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	audit-log-policy-exists(Process Check)	組織のログ要件を定義する、監査ログの管理ポリシーを確立して維持します。これには監査ログのレビューと保持が含まれますが、これらに限定されるわけではありません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
CT.DM-P8	監査およびログレコードが、ポリシーに基づき、データ最小化の原則を組み込み決定、ドキュメント化、実施、レビューされています。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
ID.DE-P2	データ処理エコシステムの関係者 (サービスプロバイダー、顧客、パートナー、製品メーカー、アプリケーション開発者など) は、プライバシーリスク評価プロセスを用いて特定され、優先順位が付けられ、評価されます。	annual-risk-assessment-performed(Process Check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P1	ID と認証情報は、承認された個人、プロセス、およびデバイスに対して発行、管理、検証、取り消し、監査されている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
PR.AC-P3	リモートアクセスが管理されている	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-P3	リモートアクセスが管理されている	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
PR.AC-P3	リモートアクセスが管理されている	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-P3	リモートアクセスが管理されている	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.AC-P3	リモートアクセスが管理されている	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
PR.AC-P3	リモートアクセスが管理されている	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P3	リモートアクセスが管理されている	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P4	最小特権と職務の分離の原則を組み込むことで、アクセス許可および認可が管理されている。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている(ネットワークの分離、ネットワークのセグメント化など)。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
PR.AC-P5	ネットワークの完全性が保護されている(ネットワークの分離、ネットワークのセグメント化など)。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメント化など)。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている(ネットワークの分離、ネットワークのセグメント化など)。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P5	ネットワークの完全性が保護されている(ネットワークの分離、ネットワークのセグメント化など)。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P6	個人とデバイスはクレデンシャルに証明され拘束され、取引のリスク (例: 個人のセキュリティやプライバシーリスク、その他の組織的リスクなど) に見合った認証が行われます。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
PR.AC-P6	個人とデバイスはクレデンシャルに証明され拘束され、取引のリスク (例: 個人のセキュリティやプライバシーリスク、その他の組織的リスクなど) に見合った認証が行われます。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P6	個人とデバイスはクレデンシャルに証明され拘束され、取引のリスク (例: 個人のセキュリティやプライバシーリスク、その他の組織的リスクなど) に見合った認証が行われます。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P6	個人とデバイスはクレデンシャルに証明され拘束され、取引のリスク (例: 個人のセキュリティやプライバシーリスク、その他の組織的リスクなど) に見合った認証が行われます。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.AC-P6	個人とデバイスはクレデンシャルに証明され拘束され、取引のリスク (例: 個人のセキュリティやプライバシーリスク、その他の組織的リスクなど) に見合った認証が行われます。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
PR.DS-P1	保管中のデータが保護されている。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
PR.DS-P1	保管中のデータが保護されている。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-P1	保管中のデータが保護されている。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
PR.DS-P1	保管中のデータが保護されている。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
PR.DS-P1	保管中のデータが保護されている。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-P1	保管中のデータが保護されている。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-P1	保管中のデータが保護されている。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-P1	保管中のデータが保護されている。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-P1	保管中のデータが保護されている。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P1	保管中のデータが保護されている。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
PR.DS-P2	転送中のデータが保護されている	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P2	転送中のデータが保護されている	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
PR.DS-P2	転送中のデータが保護されている	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P2	転送中のデータが保護されている	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
PR.DS-P2	転送中のデータが保護されている	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
PR.DS-P4	十分な容量で可用性が維持されている。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
PR.DS-P4	十分な容量で可用性が維持されている。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	バックアップ計画によって保護されたaurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
PR.DS-P4	十分な容量で可用性が維持されている。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.DS-P4	十分な容量で可用性が維持されている。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P4	十分な容量で可用性が維持されている。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
PR.DS-P5	データ漏洩に対する保護が実装されている。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。
PR.DS-P5	データ漏洩に対する保護が実装されている。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.DS-P5	データ漏洩に対する保護が実装されている。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。
PR.DS-P5	データ漏洩に対する保護が実装されている。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.DS-P5	データ漏洩に対する保護が実装されている。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
PR.DS-P5	データ漏洩に対する保護が実装されている。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.DS-P5	データ漏洩に対する保護が実装されている。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
PR.DS-P6	整合性チェックのメカニズムが、ソフトウェア、ファームウェア、および情報の整合性を検証するために使用されている。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.MA-P2	組織のアセットのリモートメンテナンスが承認され、記録され、不正アクセスを防止する方法で実行されている。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。
PR.MA-P2	組織のアセットのリモートメンテナンスが承認され、記録され、不正アクセスを防止する方法で実行されている。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P1	情報テクノロジーのベースライン設定は、セキュリティの原則 (例: 最小限の機能の概念など) を組み込んで作成および維持されている。	cloudtrail-security-trail-enabled	このルールは、複数の設定が有効になっていることをチェックすることで、 AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P1	情報テクノロジーのベースライン設定は、セキュリティの原則 (例: 最小限の機能の概念など) を組み込んで作成および維持されている。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P1	情報テクノロジーのベースライン設定は、セキュリティの原則 (例: 最小限の機能の概念など) を組み込んで作成および維持されている。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。
PR.PO-P1	情報テクノロジーのベースライン設定は、セキュリティの原則 (例: 最小限の機能の概念など) を組み込んで作成および維持されている。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P1	情報テクノロジーのベースライン設定は、セキュリティの原則 (例: 最小限の機能の概念など) を組み込んで作成および維持されている。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
PR.PO-P1	情報テクノロジーのベースライン設定は、セキュリティの原則 (例: 最小限の機能の概念など) を組み込んで作成および維持されている。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P1	情報テクノロジーのベースライン設定は、セキュリティの原則 (例: 最小限の機能の概念など) を組み込んで作成および維持されている。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P1	情報テクノロジーのベースライン設定は、セキュリティの原則 (例: 最小限の機能の概念など) を組み込んで作成および維持されている。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
AT-1: PR.PO-P10	脆弱性の管理計画が作成され、実装されている	vuln-management-plan-exists (Process Check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P2	設定の変更管理プロセスが確立され、実施されている	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。
PR.PO-P2	設定の変更管理プロセスが確立され、実施されている	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P3	情報のバックアップが実施、維持、テストされている。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PO-P7	対応計画 (インシデント対応やビジネス継続性) と復旧計画 (インシデント復旧や災害対策) が実施され、管理されている	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
PR.PO-P8	インシデント対応および復旧計画がテストされている	response-plan-tested(Process Check)	インシデント対応と復旧計画がテスト済みであることを確認します。これにより、インシデント発生時に計画が有効であるか、ギャップや更新に対処する必要があるかどうかを理解することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P2	重要な機能のみを提供するようにシステムを設定することで、最小限の機能の原則が組み込まれている。	redshift-enhanced-vpc-routing-enabled	拡張された VPC のルーティングにより、クラスターとデータリポジトリ間のすべての COPY および UNLOAD トラフィックが、Amazon VPC を通過するよう強制されます。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用してネットワークトラフィックをモニタリングすることもできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
PR.PT-P3	通信およびコントロールネットワークが保護されている。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
PR.PT-P3	通信およびコントロールネットワークが保護されている。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
PR.PT-P3	通信およびコントロールネットワークが保護されている。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
PR.PT-P3	通信およびコントロールネットワークが保護されている。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
PR.PT-P3	通信およびコントロールネットワークが保護されている。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
PR.PT-P3	通信およびコントロールネットワークが保護されている。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P3	通信およびコントロールネットワークが保護されている。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
PR.PT-P4	平常時および不都合な状況において、回復性の要件を満たすためのメカニズム (例: フェイルセーフ、ロードバランシング、ホットスワップ) が実装されている。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NIST Privacy Framework v1.0」で入手できます。

NYDFS 23 の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するよう

には設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、金融サービス会社向けのニューヨーク財務省 (NYDFS) サイバーセキュリティ要件 (23 NYCRR 500) と AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の米国の NYDFS コントロールに関連付けられます。米国の「NYDFS 23 NYCRR 500」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。		に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョンドスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (a)	(a) サイバーセキュリティプログラム 各対象エンティティは、対象エンティティの情報システムの機密性、完全性、可用性を保護するために設計されたサイバーセキュリティプログラムを維持するものとします。	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(2)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(2) 対象エンティティの情報システムと、それらの情報システムに保存されている非公開の情報を、不正なアクセス、使用、その他の悪意のある行為から保護するため、防御的なインフラストラクチャを使用してポリシーと手順を実装します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	api-gw-execution-logging-enabled	API Gateway の口グ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(3)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(3) サイバーセキュリティイベントを検知する。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
500.02 (b)(5)	(b) サイバーセキュリティプログラムは、対象エンティティのリスク評価に基づき、中核となる以下のサイバーセキュリティ機能を実行するように設計されているものとします。(5) サイバーセキュリティイベントから回復し、通常の運用とサービスを復旧する。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.05	各対象エンティティのサイバーセキュリティプログラムは、対象エンティティのリスク評価に従って開発された、対象エンティティのサイバーセキュリティプログラムの有効性を評価するために設計された監視およびテストを含むものとします。監視および試験には、継続的な監視または定期的な侵入試験および脆弱性評価を含むものとします。効果的な継続的監視、または脆弱性を生じさせるか示唆する可能性のある情報システムの変化を継続的に検出する他のシステムがない場合、対象となるエンティティは以下を実施するものとする。(a) リスク評価に基づいて特定された関連リスクに基づき、毎年決定されるエンティティの情報システムの年次侵入テスト (b) リスク評価に基	vuln-management-plan-exists (process check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	づいてエンティティの情報システムにおける公に知られたサイバーセキュリティ上の脆弱性を特定するために合理的に設計された情報システムの体系的スキャンまたはレビューなどの年2回の脆弱性アセスメント。		
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	[api-gw-execution-logging-enabled](https://aws.amazon.com/)	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (b)	(b) 各対象エンティティは、本パートのセクション 500.06 (a)(1) で要求される記録を 5 年以上維持し、本パートのセクション 500.06 (a)(2) で要求される記録を 3 年以上維持するものとします。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.06 (a)	(a) 各対象エンティティは、適用可能な範囲で、そのリスク評価に基づいてシステムを安全に維持するものとします。(1) 対象エンティティによる通常の運用と義務を十分にサポートするため、重要な金融取引を再構築するように設計されている。(2) 対象エンティティの通常の運用の重要な側面に、重大な損害を与える合理的な可能性のあるサイバーセキュリティイベントを検知し、これに対応するように設計された監査証跡が含まれている。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	ecs-task-definition-user-for-host-mode-check	タスク定義に昇格した権限がある場合は、お客様がそれらの設定に特別にオプトインしていることが原因です。このコントロールでは、タスク定義でホストネットワークが有効になっており、お客様が昇格した権限にオプトインしていない場合に、予期しない権限の昇格が発生しないかどうかを確認します。
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.07	サイバーセキュリティプログラムの一環として、各対象エンティティは、対象エンティティのリスク評価に基づき、非公開の情報へのアクセスを提供する情報システムへのユーザのアクセス許可を制限するとともに、それらのアクセス許可を定期的に見直すものとします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.8 (a)	(a) 各対象エンティティのサイバーセキュリティプログラムには、対象エンティティが利用する自社開発アプリケーションにおいて安全な開発手法を使用するために設計された書面による手順、ガイドライン、標準、および対象エンティティが利用する外部開発アプリケーションのセキュリティを対象エンティティのテクノロジー環境のコンテキストで評価、査定、またはテストするための手順が含まれるものとします。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境内に存在しないことを確認します。これらの変数をクリアテキストで保存しないでください。これらの変数をクリアテキストで保存すると、意図しないデータ漏えいや不正アクセスを招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.8 (a)	(a) 各対象エンティティのサイバーセキュリティプログラムには、対象エンティティが利用する自社開発アプリケーションにおいて安全な開発手法を使用するために設計された書面による手順、ガイドライン、標準、および対象エンティティが利用する外部開発アプリケーションのセキュリティを対象エンティティのテクノロジー環境のコンテキストで評価、査定、またはテストするための手順が含まれるものとします。	codebuild-project-source-repo-url-check	GitHub または Bitbucket ソースリポジトリ URL に、AWS Codebuild プロジェクト環境内の個人用アクセストークンとサインイン認証情報が含まれていないことを確認します。GitHub または Bitbucket リポジトリへのアクセス認可を付与するには、個人のアクセストークンまたはサインイン認証情報ではなく、OAuth を使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.09	(a) 対象となるエンティティは、本編で要求されるサイバーセキュリティプログラムの設計に情報を提供するのに十分な対象エンティティの情報システムのリスク評価を定期的に実施するものとします。当該リスク評価は、対象エンティティの情報システム、非公開情報または事業運営の変更に対処するために合理的に必要な場合には、更新されるものとします。対象となるエンティティのリスク評価は、技術開発および進化する脅威に対応するための統制の改訂を可能にし、サイバーセキュリティ、収集または保存された非公開情報、利用される情報システム、非公開情報および情報システムを保護するための統制の利用可能性と有効性に関する対象となるエンティティ	annual-risk-assessment-performed (process check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	の事業運営の特定のリスクを検討しなければなりません。		
500.12	(a) 多要素認証 各対象エンティティは、そのリスク評価に基づき、非公開の情報または情報システムへの不正なアクセスを防止するため、多要素認証またはリスクベースの認証などの効果的なコントロールを行うものとします。(b) 外部ネットワークから対象エンティティの内部ネットワークにアクセスする個人に対しては、多要素認証を使用するものとする。ただし、合理的に同等かそれ以上に安全なアクセスコントロールの使用が、対象エンティティの CISO により書面にて承認された場合はこの限りではありません。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.12	(a) 多要素認証 各対象エンティティは、そのリスク評価に基づき、非公開の情報または情報システムへの不正なアクセスを防止するため、多要素認証またはリスクベースの認証などの効果的なコントロールを行うものとします。(b) 外部ネットワークから対象エンティティの内部ネットワークにアクセスする個人に対しては、多要素認証を使用するものとする。ただし、合理的に同等かそれ以上に安全なアクセスコントロールの使用が、対象エンティティの CISO により書面にて承認された場合はこの限りではありません。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.12	(a) 多要素認証 各対象エンティティは、そのリスク評価に基づき、非公開の情報または情報システムへの不正なアクセスを防止するため、多要素認証またはリスクベースの認証などの効果的なコントロールを行うものとします。(b) 外部ネットワークから対象エンティティの内部ネットワークにアクセスする個人に対しては、多要素認証を使用するものとする。ただし、合理的に同等かそれ以上に安全なアクセスコントロールの使用が、対象エンティティの CISO により書面にて承認された場合はこの限りではありません。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.12	(a) 多要素認証 各対象エンティティは、そのリスク評価に基づき、非公開の情報または情報システムへの不正なアクセスを防止するため、多要素認証またはリスクベースの認証などの効果的なコントロールを行うものとします。(b) 外部ネットワークから対象エンティティの内部ネットワークにアクセスする個人に対しては、多要素認証を使用するものとする。ただし、合理的に同等かそれ以上に安全なアクセスコントロールの使用が、対象エンティティの CISO により書面にて承認された場合はこの限りではありません。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.12	(a) 多要素認証 各対象エンティティは、そのリスク評価に基づき、非公開の情報または情報システムへの不正なアクセスを防止するため、多要素認証またはリスクベースの認証などの効果的なコントロールを行うものとします。(b) 外部ネットワークから対象エンティティの内部ネットワークにアクセスする個人に対しては、多要素認証を使用するものとする。ただし、合理的に同等かそれ以上に安全なアクセスコントロールの使用が、対象エンティティの CISO により書面にて承認された場合はこの限りではありません。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	cloudwatch-alarm-action-check	Amazon CloudWatch アラームは、メトリクスが指定された評価期間数のしきい値を超えたときにアラームで警告します。アラームは、複数の期間にわたる閾値に対するメトリックまたはメートルの値に基づいて、1つまたは複数のアクションを実行します。このルールには、alarmActionRequired (Config デフォルト: True)、insufficientDataActionRequired (Config デフォルト: True)、okActionRequired (Config デフォルト: False) の値が必要です。実際の値には、環境に合わせたアラームのアクションを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。
500.14 (a)	(a) 権限のあるユーザーのアクティビティを監視し、権限のあるそれらのユーザーによる非公開の情報への不正なアクセスや使用、または改ざんを検知するために設計された、リスクベースのポリシー、手順、および管理を実装します。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.14 (b)	サイバーセキュリティプログラムの一環として、対象となる各エンティティは以下を行うものとします。(b) 対象となるエンティティがリスク評価で特定したリスクを反映するために更新されたサイバーセキュリティ意識向上トレーニングを、すべての人員に対して定期的に提供します。	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	codebuild-project-artifact-encryption	保管中の機密データを保護するために、AWS CodeBuild アーティファクトの暗号化が有効になっていることを確認します。
500.15 (a)	(a) サイバーセキュリティプログラムの一環として、各対象エンティティは、リスク評価に基づき、対象エンティティが保有または転送する非公開の情報を外部ネットワーク上で転送中および保管中の両方で保護するための、暗号化を含むコントロールを実装するものとします。	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
500.16	(a) サイバーセキュリティプログラムの一部として、対象となる各エンティティは、対象エンティティの情報システムの機密性、完全性もしくは可用性、または対象となるエンティティの事業もしくは運営のいかなる側面の継続的機能に重大な影響を及ぼすサイバーセキュリティ事象に迅速に対応し、そこから回復するように設計された書面による事故対応計画を策定するものとします。	response-plan-exists-maintained (process check)	インシデント対応計画が確立および維持され、責任者に配布されていることを確認します。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for NYDFS 23」で入手できます。

NZISM 3.8 の運用上のベストプラクティス

コンフォーマンスパックは、マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下は、ニュージーランド政府通信セキュリティ局 (GCSB) 情報セキュリティマニュアル (NZISM) 2022-09 バージョン 3.8 と AWS Managed Config ルール間のマッピングの例です。各 Config ルールは、特定の AWS リソースタイプに適用され、1 つ以上の NZISM コントロールに関連付けられます。「ÑZISM」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。RESTRICTED 以下に分類された情報の推奨プラクティスまたはベースラインプラクティスを表すコントロールのみがマッピングに含まれます。

このコンフォーマンスパックのサンプルテンプレートは、NZISM フレームワーク内のコントロールへのマッピングを含んでおり、これは、人員、情報および物理的セキュリティの管理に対するニュージーランド政府の期待値を定めた保護セキュリティ要件 (PSR) フレームワークの不可欠な部分です。

The NZISM is licensed under the Creative Commons Attribution 4.0 New Zealand licence, available at https://creativecommons.org/licenses/by/4.0/。著作権については、「NZISM New Zealand Information Security Manual | 法律、プライバシー、著作権」に記載されています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1149	ソフトウェアセキュリティ、標準運用環境、強化 SOEs の開発 (14.1.8.C.01)	ec2-instance-managed-by-systems-manager	Systems AWS Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケー

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
1149	ソフトウェアセキュリティ、標準運用環境、強化 SOEs の開発 (14.1.8.C.01)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations を使用して、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを支援します。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1149	ソフトウェアセキュリティ、標準運用環境、強化 SOEs の開発 (14.1.8.C.01)	ecs-containers-nonprivileged	このコントロールは、Amazon ECS タスク定義のコンテナ定義の特権パラメータが true に設定されているかどうかを確認します。このパラメータが true と等しい場合、コントロールは失敗します。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。昇格された特権を、ECS タスク定義から削除することが推奨されます。権限パラメータが true の場合、コンテナにはホストコンテナインスタンスで昇格された権限が付与されます (ルートユーザーと同様) 。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1149	ソフトウェアセキュリティ、標準運用環境、強化 SOEs の開発 (14.1.8.C.01)	ecs-containers-readonly-access	このコントロールは、Amazon ECS コンテナが、マウントされたルートファイルシステムへの読み取り専用アクセスに制限されているかどうかをチェックします。Amazon ECS タスク定義のコンテナ定義の ReadonlyRootFilesystem パラメータが false に設定されている場合、このコントロールは失敗します。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。このオプションを有効にすると、ファイルシステムフォルダとディレクトリに対する明示的な読み取り/書き込み権限がない限り、コンテナインスタンスのファイルシステムへの改ざんや書き込みができないため、セキュリティ攻撃ベクトルを減らすことができます。こ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のコントロールは、最小特権の原則にも準拠しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1661	ソフトウェアセキュリティ、ウェブアプリケーション開発、エージェンシーのウェブサイトコンテンツ (14.5.6.C.01)	cloudfront-default-root-object-configured	このコントロールは、Amazon CloudFront ディストリビューションがデフォルトのルートオブジェクトである特定のオブジェクトを返すように設定されているかどうかをチェックします。CloudFront ディストリビューションにデフォルトのルートオブジェクトが設定されていない場合、コントロールは失敗します。ユーザーは、ディストリビューション内のオブジェクトではなく、ディストリビューションのルート URL を要求することがあります。この場合、デフォルトのルートオブジェクトを指定することで、ウェブディストリビューションのコンテンツの漏洩を防止できます。このルールは us-east-1 リージョンで適用する必要があります。テンプレートパラメータ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			DeployEdgeRules = true を使用してデプロイする
1667	ソフトウェアセキュリティ、ウェブアプリケーション開発、ウェブアプリケーション (14.5.8.C.01)	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。This rule requires a value for daysToExpiration。The value is 90 days。
1667	ソフトウェアセキュリティ、ウェブアプリケーション開発、ウェブアプリケーション (14.5.8.C.01)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1841	アクセスコントロールとパスワード、識別、認証とパスワード、システムユーザー識別と認証の方法 (16.1.35.C.02)	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1841	アクセスコントロールとパスワード、識別、認証とパスワード、システムユーザー識別と認証の方法 (16.1.35.C.02)	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1841	アクセスコントロールとパスワード、識別、認証とパスワード、システムユーザー識別と認証の方法 (16.1.35.C.02)	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、AWS アカウントで最も特権のあるユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害された AWS アカウントのインシデントを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1841	アクセスコントロールとパスワード、識別、認証とパスワード、システムユーザー識別と認証の方法 (16.1.35.C.02)	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、 AWS アカウントで最も特権のあるユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害された AWS アカウントのインシデントを減らすことができます。
1847	アクセスコントロールとパスワード、識別、認証とパスワード、転送中の認証データの保護 (16.1.37.C.01)	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1847	アクセスコントロールとパスワード、識別、認証とパスワード、転送中の認証データの保護 (16.1.37.C.01)	cloudfront-viewer-policy-https	このコントロールは、Amazon CloudFront ディストリビューションで視聴者が HTTPS を直接使用する必要性、またはリダイレクトを使用するかどうかをチェックします。ViewerProtocolPolicy が defaultCacheBehavior または cacheBehaviors の allow-all に設定されている場合、コントロールは失敗します。HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。このルールは us-east-1 リージョンで適用する必要があります。テンプレートパラメータ DeployEdg

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			eRules = true を使用してデプロイする
1847	アクセスコントロールとパスワード、識別、認証とパスワード、転送中の認証データの保護 (16.1.37.C.01)	elasticsearch-node-to-node-encryption-check	このコントロールは Elasticsearch ドメインでノード間の暗号化が有効になっているかどうかをチェックします。ドメインでノード間の暗号化が無効になっている場合、このコントロールは失敗します。HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。Elasticsearch ドメインのノード間の暗号化を有効にすると、クラスター内の通信が転送中に確実に暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1847	アクセスコントロールとパスワード、識別、認証とパスワード、転送中の認証データの保護 (16.1.37.C.01)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1847	アクセスコントロールとパスワード、識別、認証とパスワード、転送中の認証データの保護 (16.1.37.C.01)	opensearch-node-to-node-encryption-check	このコントロールは、OpenSearch ドメインでノード間の暗号化が有効になっているかどうかをチェックします。ドメインでノード間の暗号化が無効になっている場合、このコントロールは失敗します。HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。OpenSearch ドメインでノード間の暗号化を有効にすると、クラスター内通信は転送中に確実に暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1858	アクセスコントロールとパスワード、識別、認証とパスワード、パスワード選択ポリシー (16.1.40.C.02.)	iam-password-policy	HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。
1893	アクセスコントロールとパスワード、識別、認証とパスワード、アクセスの停止 (16.1.46.C.02)	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge を 30 日間に設定します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1946	アクセスコントロールとパスワード、特権ユーザーアクセス、特権アカウントの使用 (16.3.5.C.02.)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「アクション」：「リソース」：「*」ではなく「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1946	アクセスコントロールとパスワード、特権ユーザーアクセス、特権アカウントの使用 (16.3.5.C.02.)	iam-root-access-key-check	システムおよびアセットへのアクセスは、ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つロールベースの AWS アカウントを作成して使用します。
1998	アクセスコントロールとパスワード、イベントログ記録と監査、システム管理ログの管理 (16.6.6.C.02)	cloud-trail-cloud-watch-logs-enabled	CloudWatch Logs で CloudTrail を使用するように設定して、証跡ログをモニタリングし、特定のアクティビティの発生時に通知を受けることができます。このルールは、 AWS CloudTrail 証跡が Amazon CloudWatch logs ログにログを送信するように設定されているかどうかを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1998	アクセスコントロールとパスワード、イベントログ記録と監査、システム管理ログの管理 (16.6.6.C.02)	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
1998	アクセスコントロールとパスワード、イベントログ記録と監査、システム管理ログの管理 (16.6.6.C.02)	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。最低保有期間は 18 ヶ月です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2013	アクセスコントロールとパスワード、イベントのログ記録と監査、記録する追加のイベント (16.6.10.C.02)	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2013	アクセスコントロールとパスワード、イベントのログ記録と監査、記録する追加のイベント (16.6.10.C.02)	cloudfront-accesslogs-enabled	このコントロールは、CloudFront ディストリビューションでサーバーアクセスのログ記録が有効になっているかどうかをチェックします。ディストリビューションでアクセスのログ記録が有効でない場合、コントロールは失敗します。CloudFront アクセスログは、CloudFront が受信するすべてのユーザーリクエストに関する詳細情報を提供します。各ログには、リクエストが受信された日時、リクエストを行ったビューワーの IP アドレス、リクエストソース、ビューワーからのリクエストポート番号などの情報が含まれます。これらのログは、セキュリティ監査やアクセス監査、証拠調査などのアプリケーションに役立ちます。このルールは us-east-1 リージョンで適用す

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			る必要があります。テンプレートパラメータ DeployEdgeRules = true を使用してデプロイする
2013	アクセスコントロールとパスワード、イベントのログ記録と監査、記録する追加のイベント (16.6.10.C.02)	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2013	アクセスコントロールとパスワード、イベントのログ記録と監査、記録する追加のイベント (16.6.10.C.02)	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
2013	アクセスコントロールとパスワード、イベントのログ記録と監査、記録する追加のイベント (16.6.10.C.02)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2013	アクセスコントロールとパスワード、イベントのログ記録と監査、記録する追加のイベント (16.6.10.C.02)	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2022	アクセスコントロールとパスワード、イベントログ記録と監査、イベントログ保護 (16.6.12.C.01.)	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
2022	アクセスコントロールとパスワード、イベントログ記録と監査、イベントログ保護 (16.6.12.C.01.)	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2028	アクセスコントロールとパスワード、イベントログ記録と監査、イベントログアーカイブ (16.6.13.C.01)	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。最低保有期間は 18 ヶ月です。
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。本番稼働前の環境では免除を受けることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	elasticsearch-encrypted-at-rest	このコントロールは、Elasticsearch ドメインでencryption-at-rest設定が有効になっているかどうかを確認します。保管中の暗号化が有効になっていない場合、チェックは失敗します。機密データのセキュリティを強化するには、保管時に暗号化されるように Elasticsearch Service ドメインを設定する必要があります。保管中のデータの暗号化を設定すると、 AWS KMS は暗号化キーを保存および管理します。暗号化を実行するために、 AWS KMS は 256 ビットキー (AES-256) で Advanced Encryption Standard アルゴリズムを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	opensearch-encrypted-at-rest	このコントロールは、OpenSearch ドメインで保管中の暗号化設定が有効になっているかどうかをチェックします。保管中の暗号化が有効になっていない場合、チェックは失敗します。機密データのセキュリティを強化するには、保管中に暗号化するように OpenSearch Service ドメインを設定する必要があります。保管中のデータの暗号化を設定すると、 AWS KMS は暗号化キーを保存および管理します。暗号化を実行するために、 AWS KMS は 256 ビットキー (AES-256) で Advanced Encryption Standard アルゴリズムを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2082	暗号化、暗号化の基礎、ストレージと物理的な転送要件の削減 (17.1.53.C.04)	s3-default-encryption-kms	保管中のデータを保護するため、S3 バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。暗号化プロセスと管理の詳細については、 AWS Key Management Service (AWS KMS) カスタマー管理 CMKs を使用します。SSE が有効になっている場合、非機密データを含むバケットには免除が適用されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2090	暗号化、暗号化の基礎、情報とシステムの保護 (17.1.55.C.02)	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2090	暗号化、暗号化の基礎、情報とシステムの保護 (17.1.55.C.02)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2090	暗号化、暗号化の基礎、情報とシステムの保護 (17.1.55.C.02)	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2598	TLS を使用した暗号化、Transport Layer Security (17.4.16.C.01)	elb-custom-security-policy-ssl-check	転送中のデータを保護するため、Classic ElasticLoadBalancer SSL のリスナーがカスタムセキュリティポリシーを使用していることを確認します。これらのポリシーは、システム間の暗号化されたネットワーク通信を実現するための、さまざまな高強度の暗号化アルゴリズムを提供します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。セキュリティポリシーは、Protocol-TLSv1.2、ECDHE-ECDSA-AES128-GCM-SHA256 です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2600	TLS を使用した暗号化、Transport Layer Security (17.4.16.C.02.)	elb-custom-security-policy-ssl-check	転送中のデータを保護するため、Classic ElasticLoadBalancer SSL のリスナーがカスタムセキュリティポリシーを使用していることを確認します。これらのポリシーは、システム間の暗号化されたネットワーク通信を実現するための、さまざまな高強度の暗号化アルゴリズムを提供します。このルールでは、SSL リスナーにカスタムセキュリティポリシーを設定する必要があります。デフォルトのセキュリティポリシーは、Protocol-TLSv1.2、ECDHE-ECDSA-AES128-GCM-SHA256 です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2726	暗号化、Secure Shell、自動リモートアクセス (17.5.8.C .02.)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの入出力ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3021	暗号化、キー管理、KMPs の内容 (17.9.25.C.01.)	cmk-backing-key-rotation-enabled	AWS KMS を使用すると、お客様はバッキングキーをローテーションできます。バッキングキーは、KMS AWS に保存されているキーマテリアルであり、CMK のキー ID に関連付けられています。バッキングキーは、暗号化や復号化などの暗号化オペレーションを実行するために使用されます。現在、キーの自動ローテーションでは以前のすべてのバッキングキーが保持されるため、暗号化したデータは透過的に復号化できます。新しいキーで暗号化されたデータは、漏洩した可能性がある以前のキーではアクセスできないため、暗号化キーをローテーションすることで、漏洩したキーにより起こる可能性のある被害を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3205	ネットワークセキュリティ、ネットワーク管理、ネットワークアクセスの制限 (18.1.13.C.02)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。許可されたインターネットポートリストは 443 のみ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3449	製品のセキュリティ、製品のパッチ適用と更新、製品の脆弱性へのパッチ適用 (12.4.4.C.02)	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3449	製品のセキュリティ、製品のパッチ適用と更新、製品の脆弱性へのパッチ適用 (12.4.4.C.02)	ecr-private-image-scanning-enabled	このコントロールは、プライベート ECR リポジトリでイメージスキャニングが設定されているかどうかをチェックします。プライベート ECR リポジトリでイメージスキャニングが設定されていないと、このコントロールは失敗します。各リポジトリがこのコントロールを渡すようにプッシュ時にスキャンを設定する必要もあることに注意してください。ECR イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR は、オープンソースの Clair プロジェクトの共通脆弱性識別子 (CVE) データベースを使用し、スキャン結果のリストを表示します。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			の整合性と安全性を検証するレイヤーが追加されます。
3449	製品のセキュリティ、製品のパッチ適用と更新、製品の脆弱性へのパッチ適用 (12.4.4.C.02)	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を TRUE に設定します。
3451	製品のセキュリティ、製品のパッチ適用と更新、製品の脆弱性へのパッチ適用 (12.4.4.C.04)	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3452	製品のセキュリティ、製品のパッチ適用と更新、製品の脆弱性へのパッチ適用 (12.4.4.C.05)	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3452	製品のセキュリティ、製品のパッチ適用と更新、製品の脆弱性へのパッチ適用 (12.4.4.C.05)	elastic-beanstalk-managed-updates-enabled	このコントロールは、Elastic Beanstalk 環境でマネージドプラットフォームの更新が有効になっているかどうかをチェックします。マネージドプラットフォームの更新を有効にすると、環境で使用可能な最新のプラットフォームの修正、更新、および機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムを保護する上で重要なステップです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3452	製品のセキュリティ、製品のパッチ適用と更新、製品の脆弱性へのパッチ適用 (12.4.4.C.05)	rds-automatic-minor-version-upgrade-enabled	このコントロールは、RDS データベースインスタンスでマイナーバージョン自動アップグレードが有効になっているかどうかをチェックします。マイナーバージョン自動アップグレードを有効にすると、リレーショナルデータベース管理システム (RDBMS) に最新のマイナーバージョンの更新がインストールされます。これらのアップグレードには、セキュリティパッチとバグ修正を含む場合があります。パッチのインストールを最新の状態に保つことは、システムを保護する上で重要なステップです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3453	製品のセキュリティ、製品のパッチ適用と更新、製品の脆弱性へのパッチ適用 (12.4.4.C.06)	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
3453	製品のセキュリティ、製品のパッチ適用と更新、製品の脆弱性へのパッチ適用 (12.4.4.C.06)	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を TRUE に設定します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。WAF が有効になっている CloudFront ディストリビューションのオリジンがロードバランサーである場合は、免除が適用されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	api-gw-associated-with-waf	このコントロールは、API Gateway ステージが AWS WAF ウェブアクセスコントロールリスト (ACL) を使用しているかどうかをチェックします。 AWS WAF リージョンウェブ ACL が REST API Gateway ステージにアタッチされていない場合、このコントロールは失敗します。 AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。これにより、ユーザーが定義するカスタマイズ可能なウェブセキュリティルールと条件に基づいて、ウェブリクエストを許可、ブロック、またはカウントする一連のルールである ACL を設定することができます。API Gateway ステージが AWS WAF ウェブ ACL に関連付けら

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			れていることを確認し、悪意のある攻撃から保護します。API Gateway が WAF が有効になっている CloudFront ディストリビューションのオリジンである場合、免除が適用されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	cloudfront-associated-with-waf	このコントロールは、CloudFront ディストリビューションが AWS WAF または AWS WAFv2 ウェブ ACLs に関連付けられているかどうかをチェックします。ディストリビューションがウェブ ACL に関連付けられていない場合、コントロールは失敗します。AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。これで、ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる一連のルールを設定することができます。このルールは、ユーザーが定義するカスタマイズ可能なウェブセキュリティルールと条件に基づいて、ウェブリクエストを許可、ブロック、またはカウントします。CloudFront ディストリ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			ビューションが AWS WAF ウェブ ACL に関連付けられていることを確認し、悪意のある攻撃から保護します。このルールは us-east-1 リージョンで適用する必要があります。テンプレートパラメータ DeployEdgeRules = true を使用してデプロイする
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。Amazon VPC 内に存在するドメインは論理的に隔離されているため、パブリックエンドポイントを使用するドメインよりも多くのセキュリティレイヤーが追加されています。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	elasticsearch-in-vpc-only	このコントロールは、Elasticsearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。Elasticsearch ドメインがパブリックサブネットに添付済みでないことを確認する必要があります。VPC 内にデプロイされた Elasticsearch ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPCs、ネットワーク ACL やセキュリティグループなど、Elasticsearch ドメインへのアクセ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			スを保護するための多数のネットワークコントロールを提供します。
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	emr-master-no-public-ip	Amazon EMR クラスターマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	opensearch-in-vpc-only	このコントロールは、OpenSearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。OpenSearch ドメインがパブリックサブネットに添付済みではないことを確認する必要があります。VPC 内にデプロイされた OpenSearch ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPC は、ネットワーク ACL やセキュリティグループを含む、OpenSearch ドメインへのアクセ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			スを安全にするため、多数のネットワークコントロールを提供します。
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls を TRUE、blockPublicPolicy を TRUE、blockPublicAcls を TRUE、restrictPublicBuckets を TRUE に設定します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、入出力ネットワークトラフィックを AWS リソースにステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3562	ゲートウェイセキュリティ、ゲートウェイ、ゲートウェイの設定 (19.1.12.C.01)	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3623	ゲートウェイセキュリティ、ゲートウェイ、非戦闘ゾーン (19.1.14.C.02)	elasticsearch-in-vpc-only	このコントロールは、Elasticsearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。Elasticsearch ドメインがパブリックサブネットに添付済みでないことを確認する必要があります。VPC 内にデプロイされた Elasticsearch ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPCs、ネットワーク ACL やセキュリティグループなど、Elasticsearch ドメインへのアクセ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			スを保護するための多数のネットワークコントロールを提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3623	ゲートウェイセキュリティ、ゲートウェイ、非戦闘ゾーン (19.1.14.C.02)	opensearch-in-vpc-only	このコントロールは、OpenSearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。OpenSearch ドメインがパブリックサブネットに添付済みではないことを確認する必要があります。VPC 内にデプロイされた OpenSearch ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPC は、ネットワーク ACL やセキュリティグループを含む、OpenSearch ドメインへのアクセ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			スを安全にするため、多数のネットワークコントロールを提供します。
3623	ゲートウェイセキュリティ、ゲートウェイ、非戦闘ゾーン (19.1.14.C.02)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3623	ゲートウェイセキュリティ、ゲートウェイ、非戦闘ゾーン (19.1.14.C.02)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。
3815	ネットワークセキュリティ、侵入の検出と防止、IDS/IPS メンテナンス (18.4.9.C.01)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3857	ネットワークセキュリティ、侵入の検出と防止、IDS/IPS の設定 (18.4.11.C.01)	guardduty-eks-protection-audit-enabled	このコントロールは、GuardDuty EKS 監査ログモニタリングが有効になっているかを確認します。GuardDuty EKS 監査ログのモニタリングは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターの疑わしいアクティビティの可能性を検出するのに役立ちます。EKS 監査ログのモニタリングは、ユーザー、Kubernetes API を使用するアプリケーション、およびコントロールプレーンからの時系列アクティビティをキャプチャします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3857	ネットワークセキュリティ、侵入の検出と防止、IDS/IPS の設定 (18.4.11.C.01)	guardduty-eks-protection-runtime-enabled	このコントロールは、自動エージェント管理による GuardDuty EKS ランタイムモニタリングが有効になっているかを確認します。Amazon GuardDuty の EKS Protection は、 AWS 環境内の Amazon EKS クラスターを保護するのに役立つ脅威検出カバレッジを提供します。EKS Runtime Monitoring は、オペレーティングシステムレベルのイベントを使用して、EKS クラスター内の EKS ノードとコンテナにおける潜在的な脅威を検出するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3857	ネットワークセキュリティ、侵入の検出と防止、IDS/IPS の設定 (18.4.11.C.01)	guardduty-lambda-protection-enabled	このコントロールは、GuardDuty Lambda Protection が有効になっているかどうかをチェックします。GuardDuty Lambda Protection は、 AWS Lambda 関数が呼び出されたときに潜在的なセキュリティ脅威を特定するのに役立ちます。Lambda Protection を有効にすると、GuardDuty は AWS アカウントの Lambda 関数に関連付けられた Lambda ネットワークアクティビティログのモニタリングを開始します。Lambda 関数が呼び出され GuardDuty が Lambda 関数に潜在的に悪意のあるコードが存在することを示す疑わしいネットワークトラフィックを特定した場合、GuardDuty は検出結果を生成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3857	ネットワークセキュリティ、侵入の検出と防止、IDS/IPS の設定 (18.4.11.C.01)	guardduty-s3-protection-enabled	このコントロールは、GuardDuty S3 Protection が有効になっているかどうかをチェックします。S3 Protection を使用すると、GuardDuty はオブジェクトレベルの API オペレーションをモニタリングして、Amazon S3 バケット内のデータの潜在的なセキュリティリスクを特定できます。GuardDuty は、AWS CloudTrail 管理イベントと CloudTrail S3 データイベントを分析して、S3 リソースに対する脅威をモニタリングします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3875	ネットワークセキュリティ、侵入の検出と防止、イベント管理と相関 (18.4.12.C.01)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3875	ネットワークセキュリティ、侵入の検出と防止、イベント管理と相関 (18.4.12.C.01)	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4333	データ管理、コンテンツフィルタリング、コンテンツ検証 (20.3.7.C.02.)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4333	データ管理、コンテンツフィルタリング、コンテンツ検証 (20.3.7.C.02.)	api-gw-associated-with-waf	このコントロールは、API Gateway ステージが AWS WAF ウェブアクセスコントロールリスト (ACL) を使用しているかどうかをチェックします。 AWS WAF リージョンウェブ ACL が REST API Gateway ステージにアタッチされていない場合、このコントロールは失敗します。 AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。これにより、ユーザーが定義するカスタマイズ可能なウェブセキュリティルールと条件に基づいて、ウェブリクエストを許可、ブロック、またはカウントする一連のルールである ACL を設定することができます。API Gateway ステージが AWS WAF ウェブ ACL に関連付けら

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			れていることを確認し、悪意のある攻撃から保護します。API Gateway が WAF が有効になっている CloudFront ディストリビューションのオリジンである場合、免除が適用されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4441	データ管理、データベース、データベースファイル (20.4.4.C.02)	elasticsearch-encrypted-at-rest	このコントロールは、Elasticsearch ドメインでencryption-at-rest設定が有効になっているかどうかを確認します。保管中の暗号化が有効になっていない場合、チェックは失敗します。機密データのセキュリティを強化するには、保管時に暗号化されるように Elasticsearch Service ドメインを設定する必要があります。保管中のデータの暗号化を設定すると、 AWS KMS は暗号化キーを保存および管理します。暗号化を実行するために、 AWS KMS は 256 ビットキー (AES-256) で Advanced Encryption Standard アルゴリズムを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4441	データ管理、データベース、データベースファイル (20.4.4.C.02)	opensearch-encrypted-at-rest	このコントロールは、OpenSearch ドメインで保管中の暗号化設定が有効になっているかどうかをチェックします。保管中の暗号化が有効になっていない場合、チェックは失敗します。機密データのセキュリティを強化するには、保管中に暗号化するように OpenSearch Service ドメインを設定する必要があります。保管中のデータの暗号化を設定すると、 AWS KMS は暗号化キーを保存および管理します。暗号化を実行するために、 AWS KMS は 256 ビットキー (AES-256) で Advanced Encryption Standard アルゴリズムを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4441	データ管理、データベース、データベースファイル (20.4.4.C.02)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
4441	データ管理、データベース、データベースファイル (20.4.4.C.02)	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4441	データ管理、データベース、データベースファイル (20.4.4.C.02)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
4441	データ管理、データベース、データベースファイル (20.4.4.C.02)	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4441	データ管理、データベース、データベースファイル (20.4.4.C.02)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、ignorePublicAcls を TRUE、blockPublicPolicy を TRUE、blockPublicAcls を TRUE、restrictPublicBuckets を TRUE に設定します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4445	データ管理、データベース、説明責任 (20.4.5.C.02.)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4445	データ管理、データベース、説明責任 (20.4.5.C.02.)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、ignorePublicAcls を TRUE、blockPublicPolicy を TRUE、blockPublicAcls を TRUE、restrictPublicBuckets を TRUE に設定します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4829	エンタープライズシステムセキュリティ、クラウドコンピューティング、システム可用性 (22.1.23.C.01)	dynamodb-autoscaling-enabled	Amazon DynamoDB 自動スケーリングは、 AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4829	エンタープライズシステムセキュリティ、クラウドコンピューティング、システム可用性 (22.1.23.C.01)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4829	エンタープライズシステムセキュリティ、クラウドコンピューティング、システム可用性 (22.1.23.C.01)	rds-cluster-multi-az-enabled	Amazon Aurora は、1 つの AWS リージョン内の複数のアベイラビリティーゾーンにまたがる DB クラスターにデータのコピーを保存します。Aurora は、DB クラスターのインスタンスが複数のアベイラビリティーゾーンにまたがっているかどうかにかかわらず、これらのコピーを作成します。データがプライマリ DB インスタンスに書き込まれると、Aurora によりアベイラビリティーゾーン全体で、クラスターボリュームに関連付けられた 6 つのストレージノードにデータが同期的に複製されます。これにより、データの冗長性が確保されて I/O のフリーズが回避され、システムバックアップ時のレイテンシー急上昇が最小限に抑えられます。高可用性を備えた DB インスタン

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			スを実行すると、計画されたシステムメンテナンス中の可用性が向上し、障害とアベイラビリティーゾーンの中断からデータベースを保護できます。このルールは、Amazon RDS によって管理される Amazon Aurora クラスタで、Multi-AZ レプリケーションが有効であるかどうかをチェックします。本番稼働前の環境では免除を受けることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4829	エンタープライズシステムセキュリティ、クラウドコンピューティング、システム可用性 (22.1.23.C.01)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。本番稼働前の環境では免除を受けることができます。
4838	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.03)	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント情報、IP アドレス、イベント発生時刻が含まれます。
4838	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.03)	ebs-snapshot-public-restorable-check	EBS スナップショットがパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4838	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.03)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls を TRUE、blockPublicPolicy を TRUE、blockPublicAcls を TRUE、restrictPublicBuckets を TRUE に設定します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4838	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.03)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
4838	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.03)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	elasticsearch-encrypted-at-rest	このコントロールは、Elasticsearch ドメインでencryption-at-rest設定が有効になっているかどうかを確認します。保管中の暗号化が有効になっていない場合、チェックは失敗します。機密データのセキュリティを強化するには、保管時に暗号化されるように Elasticsearch Service ドメインを設定する必要があります。保管中のデータの暗号化を設定すると、 AWS KMS は暗号化キーを保存および管理します。暗号化を実行するために、 AWS KMS は 256 ビットキー (AES-256) で Advanced Encryption Standard アルゴリズムを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	elasticsearch-node-to-node-encryption-check	このコントロールは Elasticsearch ドメインでノード間の暗号化が有効になっているかどうかをチェックします。ドメインでノード間の暗号化が無効になっている場合、このコントロールは失敗します。HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。Elasticsearch ドメインのノード間の暗号化を有効にすると、クラスター内の通信が転送中に確実に暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	opensearch-encrypted-at-rest	このコントロールは、OpenSearch ドメインで保管中の暗号化設定が有効になっているかどうかをチェックします。保管中の暗号化が有効になっていない場合、チェックは失敗します。機密データのセキュリティを強化するには、保管中に暗号化するように OpenSearch Service ドメインを設定する必要があります。保管中のデータの暗号化を設定すると、 AWS KMS は暗号化キーを保存および管理します。暗号化を実行するために、 AWS KMS は 256 ビットキー (AES-256) で Advanced Encryption Standard アルゴリズムを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	opensearch-node-to-node-encryption-check	このコントロールは、OpenSearch ドメインでノード間の暗号化が有効になっているかどうかをチェックします。ドメインでノード間の暗号化が無効になっている場合、このコントロールは失敗します。HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。OpenSearch ドメインでノード間の暗号化を有効にすると、クラスター内通信は転送中に確実に暗号化されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、ignorePublicAcls を TRUE、blockPublicPolicy を TRUE、blockPublicAcls を TRUE、restrictPublicBuckets を TRUE に設定します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するために、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するために、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	secretsmanager-using-cmk	保管中のデータを保護するために、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4839	エンタープライズシステムセキュリティ、クラウドコンピューティング、不正アクセス (22.1.24.C.04.)	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。トピックに発行されたメッセージに機密データが含まれていない場合は、免除が適用されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	dynamodb-in-backup-plan	データバックアッププロセスを支援するには、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。補償復旧ソリューションが設定されている場合、免除を利用できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	ebs-in-backup-plan	データバックアッププロセスを支援するには、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。補償復旧ソリューションが設定されている場合、免除を利用できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	efs-in-backup-plan	データバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。補償復旧ソリューションが設定されている場合、免除を利用できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	rds-cluster-deletion-protection-enabled	Amazon RDS インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、RDS インスタンが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	rds-in-backup-plan	データバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。補償復旧ソリューションが設定されている場合、免除を利用できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4849	エンタープライズシステムセキュリティ、クラウドコンピューティング、バックアップ、リカバリアーカイブ、データリマネンス (22.1.26.C.01)	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。免除は、オブジェクトのバリアントが 1 つだけ作成される場合、または補償復旧ソリューションが設定されている場合に使用できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6843	アクセスコントロールとパスワード、特権アクセス管理、最小特権の原則 (16.4.31.C.02)	mfa-enabled-for-iam-console-access	MFA は、ユーザーが AWS ウェブサイトやサービスにアクセスするときに、通常のサインイン認証情報に加えて、AWS がサポートする MFA メカニズムから一意の認証を提供するように要求することで、セキュリティを強化します。サポートされるメカニズムには、U2F セキュリティキー、仮想またはハードウェア MFA デバイス、SMS ベースのコードなどがあります。このルールは、コンソールパスワードを使用するすべての AWS Identity and Access Managemen t AWS Multi-Factor Authentication (MFA)) が有効になっているかどうかを確認します。MFA が有効の場合、このルールは COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6843	アクセスコントロールとパスワード、特権アクセス管理、最小特権の原則 (16.4.31.C.02)	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、AWS アカウントで最も特権のあるユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害された AWS アカウントのインシデントを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6852	アクセスコントロールとパスワード、特権アクセス管理、特権アクセス認証情報の停止と取り消し (16.4.33.C.01)	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge を 30 日間に設定します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6860	アクセスコントロールとパスワード、特権アクセス管理、モニタリングとレビュー (16.4.35.C.02.)	cloud-trail-cloud-watch-logs-enabled	CloudWatch Logs で CloudTrail を使用するように設定して、証跡ログをモニタリングし、特定のアクティビティの発生時に通知を受けることができます。このルールは、 AWS CloudTrail 証跡が Amazon CloudWatch logs ログにログを送信するように設定されているかどうかを確認します。
6860	アクセスコントロールとパスワード、特権アクセス管理、モニタリングとレビュー (16.4.35.C.02.)	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6861	アクセスコントロールとパスワード、特権アクセス管理、モニタリングとレビュー (16.4.35.C.03)	cloudtrail-security-trail-enabled	このルールは、複数の設定の有効化をチェックすることで、AWS CloudTrail に AWS 推奨されるセキュリティのベストプラクティスを確実に使用するのに役立ちます。これには、ログ暗号化の使用、ログの検証、複数のリージョンでの AWS CloudTrail の有効化が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6953	アクセスコントロールとパスワード、多要素認証、システムアーキテクチャとセキュリティコントロール (16.7.34.C.02.)	mfa-enabled-for-iam-console-access	MFA は、ユーザーが AWS ウェブサイトやサービスにアクセスするときに、通常のサインイン認証情報に加えて、AWS がサポートする MFA メカニズムから一意の認証を提供するように要求することで、セキュリティを強化します。サポートされるメカニズムには、U2F セキュリティキー、仮想またはハードウェア MFA デバイス、SMS ベースのコードなどがあります。このルールは、コンソールパスワードを使用するすべての AWS Identity and Access Managemen t AWS Multi-Factor Authentication (MFA)) が有効になっているかどうかを確認します。MFA が有効の場合、このルールは COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6953	アクセスコントロールとパスワード、多要素認証、システムアーキテクチャとセキュリティコントロール (16.7.34.C.02.)	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、AWS アカウントで最も特権のあるユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害された AWS アカウントのインシデントを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7436	パブリッククラウドセキュリティ、ID 管理とアクセスコントロール、ユーザー名とパスワード (23.3.19.C.01)	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7436	パブリッククラウドセキュリティ、ID 管理とアクセスコントロール、ユーザー名とパスワード (23.3.19.C.01)	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7436	パブリッククラウドセキュリティ、ID 管理とアクセスコントロール、ユーザー名とパスワード (23.3.19.C.01)	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、AWS アカウントで最も特権のあるユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害された AWS アカウントのインシデントを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7436	パブリッククラウドセキュリティ、ID 管理とアクセスコントロール、ユーザー名とパスワード (23.3.19.C.01)	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、 AWS アカウントで最も特権のあるユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害された AWS アカウントのインシデントを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7437	パブリッククラウドセキュリティ、ID 管理とアクセスコントロール、ユーザー名とパスワード (23.3.19.C.01)	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべての IAM ユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7437	パブリッククラウドセキュリティ、ID 管理とアクセスコントロール、ユーザー名とパスワード (23.3.19.C.01)	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。IAM ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7437	パブリッククラウドセキュリティ、ID 管理とアクセスコントロール、ユーザー名とパスワード (23.3.19.C.01)	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、AWS アカウントで最も特権のあるユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害された AWS アカウントのインシデントを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7437	パブリッククラウドセキュリティ、ID 管理とアクセスコントロール、ユーザー名とパスワード (23.3.19.C.01)	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、 AWS アカウントで最も特権のあるユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害された AWS アカウントのインシデントを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	api-gw-associated-with-waf	このコントロールは、API Gateway ステージが AWS WAF ウェブアクセスコントロールリスト (ACL) を使用しているかどうかをチェックします。 AWS WAF リージョンウェブ ACL が REST API Gateway ステージにアタッチされていない場合、このコントロールは失敗します。 AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。これにより、ユーザーが定義するカスタマイズ可能なウェブセキュリティルールと条件に基づいて、ウェブリクエストを許可、ブロック、またはカウントする一連のルールである ACL を設定することができます。API Gateway ステージが AWS WAF ウェブ ACL に関連付けら

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			れていることを確認し、悪意のある攻撃から保護します。API Gateway が WAF が有効になっている CloudFront ディストリビューションのオリジンである場合、免除が適用されます。
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。Amazon VPC 内に存在するドメインは論理的に隔離されているため、パブリックエンドポイントを使用するドメインよりも多くのセキュリティレイヤーが追加されています。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	elasticsearch-in-vpc-only	このコントロールは、Elasticsearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。Elasticsearch ドメインがパブリックサブネットに添付済みでないことを確認する必要があります。VPC 内にデプロイされた Elasticsearch ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPCs、ネットワーク ACL やセキュリティグループなど、Elasticsearch ドメインへのアクセ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			スを保護するための多数のネットワークコントロールを提供します。
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	emr-master-no-public-ip	Amazon EMR クラスターマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを特定するための悪意のある IPs と機械学習のリストが含まれます。
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	opensearch-in-vpc-only	このコントロールは、OpenSearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。OpenSearch ドメインがパブリックサブネットに添付済みではないことを確認する必要があります。VPC 内にデプロイされた OpenSearch ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPC は、ネットワーク ACL やセキュリティグループを含む、OpenSearch ドメインへのアクセ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			スを安全にするため、多数のネットワークコントロールを提供します。
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls を TRUE、blockPublicPolicy を TRUE、blockPublicAcls を TRUE、restrictPublicBuckets を TRUE に設定します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、入出力ネットワークトラフィックを AWS リソースにステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7466	パブリッククラウドセキュリティ、パブリッククラウドでのデータ保護、データアクセシビリティ (23.4.10.C.01.)	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
7496	Public Cloud Security、Logging and Alerting in Public Cloud、Logging requirements (23.5.11.C.01)	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7496	Public Cloud Security、Logging and Alerting in Public Cloud、Logging requirements (23.5.11.C.01)	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7496	Public Cloud Security、Logging and Alerting in Public Cloud、Logging requirements (23.5.11.C.01)	cloudfront-accesslogs-enabled	このコントロールは、CloudFront ディストリビューションでサーバーアクセスのログ記録が有効になっているかどうかをチェックします。ディストリビューションでアクセスのログ記録が有効でない場合、コントロールは失敗します。CloudFront アクセスログは、CloudFront が受信するすべてのユーザーリクエストに関する詳細情報を提供します。各ログには、リクエストが受信された日時、リクエストを行ったビューワーの IP アドレス、リクエストソース、ビューワーからのリクエストポート番号などの情報が含まれます。これらのログは、セキュリティ監査やアクセス監査、証拠調査などのアプリケーションに役立ちます。このルールは us-east-1

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			リージョンで適用する必要があります。
7496	Public Cloud Security、Logging and Alerting in Public Cloud、Logging requirements (23.5.11.C.01)	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出したユーザーと AWS アカウント、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
7496	Public Cloud Security、Logging and Alerting in Public Cloud、Logging requirements (23.5.11.C.01)	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7496	Public Cloud Security、Logging and Alerting in Public Cloud、Logging requirements (23.5.11.C.01)	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
7496	Public Cloud Security、Logging and Alerting in Public Cloud、Logging requirements (23.5.11.C.01)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7496	Public Cloud Security、Logging and Alerting in Public Cloud、Logging requirements (23.5.11.C.01)	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for 」で入手できます。

PCI DSS 3.2.1 運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 と AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の PCI DSS コントロールに関連付けられます。「PCI DSS」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	alb-desync-mode-check	HTTP Desync の脆弱性からアプリケーションを保護するには、アプリケーションロードバランサーで HTTP Desync 軽減モードが有効になっていることを確認してください。HTTP Desync の問題はリクエストスマグリングにつながり、アプリケーションがリクエストキューやキャッシュポイズニングに対して脆弱になる可能性があります。Desync 軽減モードの種類は、モニタリングモード、防御モード、厳密モードです。防御モードがデフォルトです。
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	のパブリックアクセスを禁止します。		します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	netfw-stateless-rule-group-not-empty	AWS Network Firewall ルールグループには、ファイアウォールが VPC 内のトラフィックを処理する方法を定義するルールが含まれています。ファイアウォールポリシーに空のステートレスルールグループが存在する場合、トラフィックは処理されません。
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3	インターネットとカード会員データ環境のシステムコンポーネントとの間の直接のパブリックアクセスを禁止します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	netfw-policy-rule-group-associated	AWS Network Firewall ポリシーは、ファイアウォールが Amazon VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定して、パケットとトラフィックフローのフィルタリングし、デフォルトのトラフィック処理を定義します。
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	netfw-stateless-rule-group-not-empty	AWS Network Firewall ルールグループには、ファイアウォールが VPC 内のトラフィックを処理する方法を定義するルールが含まれています。ファイアウォールポリシーに空のステートレスルールグループが存在する場合、トラフィックは処理されません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.6	カード所有者データを保存するシステムコンポーネント (データベースなど) は、内部ネットワークゾーン内に、DMZ およびその他の信頼されていないネットワークから分離して配置します。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1	ネットワークにシステムをインストールする前に、ベンダーが提供するデフォルト設定を必ず変更し、不要なデフォルトアカウントを削除または無効にします。これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーションおよびシステムアカウント、POS端末、決済アプリケーション、SNMP (Simple Network Management Protocol) コミュニティ文字列など、すべてのデフォルトパスワードに適用されます)。	rds-cluster-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Relational Database Service (Amazon RDS) データベースクラスターのアタックサーフェスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1	ネットワークにシステムをインストールする前に、ベンダーが提供するデフォルト設定を必ず変更し、不要なデフォルトアカウントを削除または無効にします。これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーションおよびシステムアカウント、POS端末、決済アプリケーション、SNMP (Simple Network Management Protocol) コミュニティ文字列など、すべてのデフォルトパスワードに適用されます)。	rds-instance-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Relational Database Service (Amazon RDS) データベースインスタンスのアタックサーフェスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1	ネットワークにシステムをインストールする前に、ベンダーが提供するデフォルト設定を必ず変更し、不要なデフォルトアカウントを削除または無効にします。これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーションおよびシステムアカウント、POS端末、決済アプリケーション、SNMP (Simple Network Management Protocol) コミュニティ文字列など、すべてのデフォルトパスワードに適用されます)。	redshift-default-admin-check	デフォルトのユーザー名はパブリックナレッジであるため、デフォルトのユーザー名を変更することで、Amazon Redshift クラスターのアタックサーフェスを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1	ネットワークにシステムをインストールする前に、ベンダーが提供するデフォルト設定を必ず変更し、不要なデフォルトアカウントを削除または無効にします。これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーションおよびシステムアカウント、POS端末、決済アプリケーション、SNMP (Simple Network Management Protocol) コミュニティ文字列など、すべてのデフォルトパスワードに適用されます)。	redshift-default-db-name-check	デフォルトの名前は一般に知られているため、設定時に変更する必要があります。Amazon Redshift クラスターのデフォルトのデータベース名を変更することで、Redshift クラスターの攻撃面を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1	ネットワークにシステムをインストールする前に、ベンダーが提供するデフォルト設定を必ず変更し、不要なデフォルトアカウントを削除または無効にします。これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーションおよびシステムアカウント、POS端末、決済アプリケーション、SNMP (Simple Network Management Protocol) コミュニティ文字列など、すべてのデフォルトパスワードに適用されます)。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.1	ネットワークにシステムをインストールする前に、ベンダーが提供するデフォルト設定を必ず変更し、不要なデフォルトアカウントを削除または無効にします。これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーションおよびシステムアカウント、POS端末、決済アプリケーション、SNMP (Simple Network Management Protocol) コミュニティ文字列など、すべてのデフォルトパスワードに適用されます)。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	account-part-of-organizations	AWS Organizations AWS アカウント 内のの一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	ec2-instance-multiple-eni-check	このルールは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに複数の ENI があるかどうかを確認します。複数の ENI が存在すると、デュアルホームインスタンス (複数のサブネットを持つインスタンス) を引き起こす可能性があります。これにより、ネットワークセキュリティの複雑性が増し、意図しないネットワークパスとアクセスが導入する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。Ä¢ インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)、Ä¢ SysAdmin Audit Network Security (SANS) Institute Ä¢・国立標準技術研究所 (NIST)。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。Ä¢ インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)、Ä¢ SysAdmin Audit Network Security (SANS) Institute Ä¢・国立標準技術研究所 (NIST)。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2	すべてのシステムコンポーネントに対する設定の標準を作成します。この基準は、すべての既知のセキュリティ脆弱性に対処し、業界で受け入れられているシステム強化基準に準拠するものである必要がある。業界で受け入れられているシステムハードニング標準の情報源は、以下に限定されるものではありません。・インターネットセキュリティセンター (CIS)・国際標準化機構 (ISO)・Sys Admin Audit Network Security (SANS) Institute・国立標準技術研究所 (NIST)。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.2	システムの機能に必要なサービス、プロトコル、デーモンのみを有効にします。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.3	安全ではないと考えられる必要なサービス、プロトコル、またはデーモンには、追加のセキュリティ機能を実装します。	alb-desync-mode-check	HTTP Desync の脆弱性からアプリケーションを保護するには、アプリケーションロードバランサーで HTTP Desync 軽減モードが有効になっていることを確認してください。HTTP Desync の問題はリクエストスマグリングにつながり、アプリケーションがリクエストキューやキャッシュポイズニングに対して脆弱になる可能性があります。Desync 軽減モードの種類は、モニタリングモード、防御モード、厳密モードです。防御モードがデフォルトです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.3	コンソール以外の管理者アクセスは、強力な暗号を使用して暗号化します。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
2.3	コンソール以外の管理者アクセスは、強力な暗号を使用して暗号化します。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
2.3	コンソール以外の管理者アクセスは、強力な暗号を使用して暗号化します。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.3	コンソール以外の管理者アクセスは、強力な暗号を使用して暗号化します。	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
2.3	コンソール以外の管理者アクセスは、強力な暗号を使用して暗号化します。	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.4	PCI DSS の対象となるシステムコンポーネントのインベントリを管理します。	ec2-security-group-attached-to-eni-periodic	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは ENI にセキュリティグループがアタッチされるようになります。このルールは、インベントリ内の未使用のセキュリティグループのモニタリングと環境の管理に役立ちます。
2.4	PCI DSS の対象となるシステムコンポーネントのインベントリを管理します。	eip-attached	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) に割り当てられた Elastic IP が、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは使用中の Elastic Network Interface にアタッチされるようになります。このルールは、環境内の未使用の EIP をモニタリングするのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.4	PCI DSS の対象となるシステムコンポーネントのインベントリを管理します。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.4	PCI DSS の対象となるシステムコンポーネントのインベントリを管理します。	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1	すべてのカード会員データ (CHD) の保管について、少なくとも以下を含むデータ保持および廃棄のポリシー、手順、およびプロセスを導入することにより、カード会員データの保管を最小限に抑える。・ データの保存量と保存期間を、法律、規制、および/またはビジネス要件に必要な範囲に制限する・ カード会員データの特定の保存要件・ 不要になったデータを安全に削除するプロセス・ 四半期ごとに、保存期間が規定値を超えたカード会員データを特定し、安全に削除するプロセス。	s3-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1	すべてのカード会員データ (CHD) の保管について、少なくとも以下を含むデータ保持および廃棄のポリシー、手順、およびプロセスを導入することにより、カード会員データの保管を最小限に抑える。・ データの保存量と保存期間を、法律、規制、および/またはビジネス要件に必要な範囲に制限する・ カード会員データの特定の保存要件・ 不要になったデータを安全に削除するプロセス・ 四半期ごとに、保存期間が規定値を超えたカード会員データを特定し、安全に削除するプロセス。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
3.1	すべてのカード会員データ (CHD) の保管について、少なくとも以下を含むデータ保持および廃棄のポリシー、手順、およびプロセスを導入することにより、カード会員データの保管を最小限に抑える。・データの保存量と保存期間を、法律、規制、および/またはビジネス要件に必要な範囲に制限する・カード会員データの特定の保存要件・不要になったデータを安全に削除するプロセス・四半期ごとに、保存期間が規定値を超えたカード会員データを特定し、安全に削除するプロセス。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1	すべてのカード会員データ (CHD) の保管について、少なくとも以下を含むデータ保持および廃棄のポリシー、手順、およびプロセスを導入することにより、カード会員データの保管を最小限に抑える。・ データの保存量と保存期間を、法律、規制、および/またはビジネス要件に必要な範囲に制限する・ カード会員データの特定の保存要件・ 不要になったデータを安全に削除するプロセス・ 四半期ごとに、保存期間が規定値を超えたカード会員データを特定し、安全に削除するプロセス。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.4	以下のいずれかの方法を用いて、PAN が保存されている場所 (ポータブルデジタルメディア、バックアップメディア、ログを含む) を読み取り不能にすること。・強力な暗号に基づく一方向ハッシュ (ハッシュは PAN 全体でなければならない)・切り捨て(切り捨てられた部分の PAN を置き換えるためにハッシュは使用できない)・インデックストークンおよびパッド(パッドは安全に保管しなければならない)・関連するキー管理プロセスおよび手続きを伴う強力な暗号。注: 悪意のある個人が、PAN の切り捨てバージョンとハッシュ化バージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業です。同じ PAN のハッシュ化バージョンとトラン	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
	ケートバージョンがエンティティ 環境に存在する場合、元の PAN を再構築するためにハッシュ化バージョンとトランケートバージョンを関連付けることができないように、追加の管理体制を整える必要があります。		

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.2	暗号キーへアクセスできるのは、必要最小限の管理者に制限します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.2	暗号キーへアクセスできるのは、必要最小限の管理者に制限します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.3	カード会員データの暗号化/復号化に使用されるシークレットキーとプライベートキーは、常に次の形式のいずれか (または複数) で保管してください。• データ暗号化キーと少なくとも同等の強度を持つキー暗号化キーで暗号化し、データ暗号化キーとは別に保管する • 安全な暗号化方式でデバイス (ハードウェア (ホストなど) セキュリティモジュール (HSM) や PTS が承認したポイントオブインタラクションデバイスなど)内にあること • 業界で認められている方法に従って、少なくとも 2 つのフルレングスのキーコンポーネントまたはキーシェアとして使用します。注意: パブリックキーをこれらのいずれかの形式で保存する必要はありません。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.3	カード会員データの暗号化/復号化に使用されるシークレットキーとプライベートキーは、常に次の形式のいずれか (または複数) で保管してください。• データ暗号化キーと少なくとも同等の強度を持つキー暗号化キーで暗号化し、データ暗号化キーとは別に保管する • 安全な暗号化方式でデバイス (ハードウェア (ホストなど) セキュリティモジュール (HSM) や PTS が承認したポイントオブインタラクションデバイスなど)内にあること • 業界で認められている方法に従って、少なくとも 2 つのフルレングスのキーコンポーネントまたはキーシェアとして使用します。注意: パブリックキーをこれらのいずれかの形式で保存する必要はありません。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.3	カード会員データの暗号化/復号化に使用されるシークレットキーとプライベートキーは、常に次の形式のいずれか (または複数) で保管してください。• データ暗号化キーと少なくとも同等の強度を持つキー暗号化キーで暗号化し、データ暗号化キーとは別に保管する • 安全な暗号化方式でデバイス (ハードウェア (ホストなど) セキュリティモジュール (HSM) や PTS が承認したポイントオブインタラクションデバイスなど)内にあること • 業界で認められている方法に従って、少なくとも 2 つのフルレングスのキーコンポーネントまたはキーシェアとして使用します。注意: パブリックキーをこれらのいずれかの形式で保存する必要はありません。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.4	関連するアプリケーション・ベンダーまたはキーの所有者によって定義され、業界のベストプラクティスおよびガイドライン(NIST Special Publication 800-57 など)に基づく、暗号期間の終了に達した鍵の 変更 (例えば、定められた期間が経過した後および/または所定の鍵によって一定量の暗号文が生成された後など)。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.5	キーの完全性が損なわれた場合 (例えば、平文のキーコンポーネントを知っている従業員が退職した場合)、またはキーが危険にさらされている疑いがある場合は、必要と思われるキーの廃棄または交換 (アーカイブ、破棄、取り消しなど)。注意: 廃止または交換された暗号化キーを保存する必要がある場合は、これらの鍵を (キー暗号化キーを使用するなどして) 安全にアーカイブする必要があります。アーカイブされた暗号化キーは、復号化/検証の目的でのみ使用してください。	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.7	暗号化キーの不正な代替の防止	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.1	強力な暗号化テクノロジーとセキュリティプロトコルを使用して、以下のようにオープンパブリックなネットワークを介して転送される機密性の高いカード会員データを保護します。・ 信頼できるキーおよび証明書のみを使用する。• 使用中のプロトコルは、安全なバージョンまたは設定のみをサポートしています。• 暗号化強度は、使用する暗号化方式に適したものです。オープンでパブリックなネットワークの例としては、これらに限定されるものではありません。・ インターネット・ 無線技術 (802.11、Bluetooth など)・ GSM、CDMA などの携帯電話技術・ GPRS (一般パケット無線サービス)・ 衛星通信	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.2	ベンダーが提供する該当するセキュリティパッチをインストールして、すべてのシステムコンポーネントとソフトウェアが既知の脆弱性から保護されていることを確認します。重要なセキュリティパッチは、公開から 1 か月以内にインストールする。注: 重要なセキュリティパッチは、要件 6.1 で定義されたリスクランキングプロセスに従って特定する必要があります。	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.2	ベンダーが提供する該当するセキュリティパッチをインストールして、すべてのシステムコンポーネントとソフトウェアが既知の脆弱性から保護されていることを確認します。重要なセキュリティパッチは、公開から 1 か月以内にインストールする。注: 重要なセキュリティパッチは、要件 6.1 で定義されたリスクランキングプロセスに従って特定する必要があります。	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.2	ベンダーが提供する該当するセキュリティパッチをインストールして、すべてのシステムコンポーネントとソフトウェアが既知の脆弱性から保護されていることを確認します。重要なセキュリティパッチは、公開から 1 か月以内にインストールする。注: 重要なセキュリティパッチは、要件 6.1 で定義されたリスクランキングプロセスに従って特定する必要があります。	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.2	ベンダーが提供する該当するセキュリティパッチをインストールして、すべてのシステムコンポーネントとソフトウェアが既知の脆弱性から保護されていることを確認します。重要なセキュリティパッチは、公開から 1 か月以内にインストールする。注: 重要なセキュリティパッチは、要件 6.1 で定義されたリスクランキングプロセスに従って特定する必要があります。	ecs-fargate-latest-platform-version	セキュリティの更新とパッチは、 AWS Fargate タスクに自動的にデプロイされます。 AWS Fargate プラットフォームのバージョンに影響するセキュリティ上の問題が見つかった場合、 はプラットフォームのバージョンを AWS パッチします。 AWS Fargate を実行する Amazon Elastic Container Service (ECS) タスクのパッチ管理を支援するために、サービスのスタンドアロンタスクを更新して最新のプラットフォームバージョンを使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.2	ベンダーが提供する該当するセキュリティパッチをインストールして、すべてのシステムコンポーネントとソフトウェアが既知の脆弱性から保護されていることを確認します。重要なセキュリティパッチは、公開から 1 か月以内にインストールする。注: 重要なセキュリティパッチは、要件 6.1 で定義されたリスクランキングプロセスに従って特定する必要があります。	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.2	ベンダーが提供する該当するセキュリティパッチをインストールして、すべてのシステムコンポーネントとソフトウェアが既知の脆弱性から保護されていることを確認します。重要なセキュリティパッチは、公開から 1 か月以内にインストールする。注: 重要なセキュリティパッチは、要件 6.1 で定義されたリスクランキングプロセスに従って特定する必要があります。	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3.2	(手動または自動プロセスのいずれかを使用して) 潜在的なコーディングの脆弱性を特定するために、本番環境または顧客にリリースする前にカスタムコードをレビューします。• コードの変更は、元のコード作成者以外の個人、およびコードレビュー技術と安全なコーディングプラクティスに精通している個人によってレビューされます。• コードレビューにより、コードが安全なコーディングガイドラインに従って開発されていることを確認します。• リリース前に適切な修正が実施されます。• コードレビューの結果は、リリース前に管理者によってレビューおよび承認されます。(次のページに続く)	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.6	公開用ウェブアプリケーションについては、以下のいずれかの方法により、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが既知の攻撃から保護されていることを確認します。・ 手動または自動のアプリケーション脆弱性セキュリティ評価ツールまたは手法から、少なくとも年 1 回、および変更後に、公開用 Web アプリケーションをレビューします (注: この評価は、要件 11.2 で実施した脆弱性スキャンとは異なります)。・ ウェブベースの攻撃を検知・防止する自動化された技術ソリューション (例: ウェブアプリケーションファイアウォール) を公衆向けウェブアプリケーションの前に設置し、すべてのトラフィックを継続的にチェックします。	alb-desync-mode-check	HTTP Desync の脆弱性からアプリケーションを保護するには、アプリケーションロードバランサーで HTTP Desync 軽減モードが有効になっていることを確認してください。HTTP Desync の問題はリクエストスマグリングにつながり、アプリケーションがリクエストキューやキャッシュポイズニングに対して脆弱になる可能性があります。Desync 軽減モードの種類は、モニタリングモード、防御モード、厳密モードです。防御モードがデフォルトです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.6	公開用ウェブアプリケーションについては、以下のいずれかの方法により、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが既知の攻撃から保護されていることを確認します。・ 手動または自動のアプリケーション脆弱性セキュリティ評価ツールまたは手法から、少なくとも年 1 回、および変更後に、公開用 Web アプリケーションをレビューします (注: この評価は、要件 11.2 で実施した脆弱性スキャンとは異なります)。・ ウェブベースの攻撃を検知・防止する自動化された技術ソリューション (例: ウェブアプリケーションファイアウォール) を公衆向けウェブアプリケーションの前に設置し、すべてのトラフィックを継続的にチェックします。	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.6	公開用ウェブアプリケーションについては、以下のいずれかの方法により、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが既知の攻撃から保護されていることを確認します。・ 手動または自動のアプリケーション脆弱性セキュリティ評価ツールまたは手法から、少なくとも年 1 回、および変更後に、公開用 Web アプリケーションをレビューします (注: この評価は、要件 11.2 で実施した脆弱性スキャンとは異なります)。・ ウェブベースの攻撃を検知・防止する自動化された技術ソリューション (例: ウェブアプリケーションファイアウォール) を公衆向けウェブアプリケーションの前に設置し、すべてのトラフィックを継続的にチェックします。	[api-gw-associated-with-waf](#)	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.6	公開用ウェブアプリケーションについては、以下のいずれかの方法により、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが既知の攻撃から保護されていることを確認します。・ 手動または自動のアプリケーション脆弱性セキュリティ評価ツールまたは手法から、少なくとも年 1 回、および変更後に、公開用 Web アプリケーションをレビューします (注: この評価は、要件 11.2 で実施した脆弱性スキャンとは異なります)。・ ウェブベースの攻撃を検知・ 防止する自動化された技術ソリューション (例: ウェブアプリケーションファイアウォール) を公衆向けウェブアプリケーションの前に設置し、すべてのトラフィックを継続的にチェックします。	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.6	公開用ウェブアプリケーションについては、以下のいずれかの方法により、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが既知の攻撃から保護されていることを確認します。・ 手動または自動のアプリケーション脆弱性セキュリティ評価ツールまたは手法から、少なくとも年 1 回、および変更後に、公開用 Web アプリケーションをレビューします (注: この評価は、要件 11.2 で実施した脆弱性スキャンとは異なります)。・ ウェブベースの攻撃を検知・防止する自動化された技術ソリューション (例: ウェブアプリケーションファイアウォール) を公衆向けウェブアプリケーションの前に設置し、すべてのトラフィックを継続的にチェックします。	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.6	公開用ウェブアプリケーションについては、以下のいずれかの方法により、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが既知の攻撃から保護されていることを確認します。・ 手動または自動のアプリケーション脆弱性セキュリティ評価ツールまたは手法から、少なくとも年 1 回、および変更後に、公開用 Web アプリケーションをレビューします (注: この評価は、要件 11.2 で実施した脆弱性スキャンとは異なります)。・ ウェブベースの攻撃を検知・ 防止する自動化された技術ソリューション (例: ウェブアプリケーションファイアウォール) を公衆向けウェブアプリケーションの前に設置し、すべてのトラフィックを継続的にチェックします。	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。 ・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。
7.1.1	各役割のアクセスニーズを定義します。・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。
7.1.1	各役割のアクセスニーズを定義します。・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。 ・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。 ・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。 ・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。 ・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（ AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。・各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
7.1.1	各役割のアクセスニーズを定義します。・各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。 ・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
7.1.1	各役割のアクセスニーズを定義します。・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.1	各役割のアクセスニーズを定義します。 ・ 各役割が職務上アクセスする必要のあるシステムコンポーネントおよびデータリソース・ リソースへのアクセスに必要な権限のレベル (例: ユーザー、管理者等)。	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.2	特権的ユーザーの ID へのアクセスを、職務の遂行に必要な最小限の権限に制限します。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーでブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.2	特権的ユーザーの ID へのアクセスを、職務の遂行に必要な最小限の権限に制限します。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.2	特権的ユーザーの ID へのアクセスを、職務の遂行に必要な最小限の権限に制限します。	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.2	特権的ユーザーの ID へのアクセスを、職務の遂行に必要な最小限の権限に制限します。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.2	特権的ユーザーの ID へのアクセスを、職務の遂行に必要な最小限の権限に制限します。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
7.1.2	特権的ユーザーの ID へのアクセスを、職務の遂行に必要な最小限の権限に制限します。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.2	特権的ユーザーの ID へのアクセスを、職務の遂行に必要な最小限の権限に制限します。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.1.2	特権的ユーザーの ID へのアクセスを、職務の遂行に必要な最小限の権限に制限します。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
7.1.2	特権的ユーザーの ID へのアクセスを、職務の遂行に必要な最小限の権限に制限します。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムには、以下のものが含まれている必要があります。すべてのシステムコンポーネントのカバレッジ	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	ecs-containers-nonprivileged	最小特権の原則の実装を支援するため、Amazon Elastic Container Service (Amazon ECS) タスク定義では拡張された特権を有効にしないでください。このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (ルートユーザーと同様) が付与されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	ecs-containers-readonly-access	Amazon Elastic Container Service (Amazon ECS) コンテナへの読み取り専用アクセスを有効にすると、最小特権のプリンシパルを遵守するのに役立ちます。このオプションにより、明示的な読み取り/書き込み権限がない場合にはコンテナインスタンスのファイルシステムを変更できないため、攻撃ベクトルを減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントについて、ユーザーに必要な情報に基づいてアクセスを制限し、特に許可されていない限り「すべて拒否」に設定されているシステムコンポーネントのアクセスコントロールシステムを確立します。このアクセスコントロールシステムは、以下を含む必要があります: Assignment of privileges to individuals based on job classification and function	opensearch-access-control-enabled	Amazon OpenSearch Service ドメインで、きめ細かいアクセスコントロールが有効になっていることを確認します。きめ細かいアクセスコントロールによって、Amazon OpenSearch Service ドメインへの最小特権アクセスを実現するための強化された認可メカニズムが得られます。これにより、ドメインへのロールベースのアクセスコントロール、インデックス、ドキュメント、およびフィールドレベルのセキュリティ、Open Search Service ダッシュボードのマルチテナンシーのサポート、OpenSearch Service と Kibana の HTTP 基本認証が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.3	デフォルトの「すべて拒否」設定。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1.1	システムコンポーネントまたはカード会員データへのアクセスを許可する前に、すべてのユーザーに一意の ID を割り当てます。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1.4	非アクティブなユーザーアカウントを 90 日以内に削除/無効にします。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	codebuild-project-environment-privileged-check	最小特権の原則の実装を支援するために、Amazon CodeBuild プロジェクト環境で特権モードが有効になっていないことを確認してください。Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	ecs-no-environment-secrets	セキュリティ上のベストプラクティスとして、機密情報を環境変数としてコンテナに渡します。Amazon ECS タスク定義のコンテナ定義で AWS Systems Manager パラメータストアまたは AWS Secrets Manager に保存されている値を参照することで、Amazon Elastic Container Service (ECS) コンテナにデータを安全に挿入できます。次に、機密情報を環境変数として、またはコンテナのログ設定で公開できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	強力な暗号化を使用して、すべてのシステムコンポーネントの転送中および保管中に、すべての認証情報 (パスワード/フレーズなど) の読み取りができないようにレンダリングします。	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.3	パスワード/パスフレーズは、以下を満たす必要があります: • 最低でも 7 文字以上の長さを必要とする。• 数字とアルファベットの両方が含まれている。あるいは、パスワード/パスフレーズは、少なくとも上記で指定されたパラメータと同等の複雑さと強度を有していなければなりません。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、IAM パスワードポリシーの RequireUppercaseCharacters (PCI DSSデフォルト: false)、RequireLowercaseCharacters (PCI DSS デフォルト: true)、RequireSymbols (PCI DSS デフォルト: false)、RequireNumbers (PCI DSSデフォルト: true)、MinimumPasswordLength (PCI DSSデフォルト: 7)、PasswordReusePrevention (PCI DSSデフォルト: 4)、MaxPasswordAge (PCI DSS デフォルト: 90) を、必要に応じ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			て設定することができます。実際の値には、組織のポリシーを反映する必要があります。
8.2.4	ユーザーのパスワード/パスフレーズは、少なくとも90 日ごとに変更します。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.4	ユーザーのパスワード/パスフレーズは、少なくとも90 日ごとに変更します。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、IAM パスワードポリシーの RequireUppercaseCharacters (PCI DSSデフォルト: false)、RequireLowercaseCharacters (PCI DSS デフォルト: true)、RequireSymbols (PCI DSS デフォルト: false)、RequireNumbers (PCI DSSデフォルト: true)、MinimumPasswordLength (PCI DSSデフォルト: 7)、PasswordReusePrevention (PCI DSSデフォルト: 4)、MaxPasswordAge (PCI DSS デフォルト: 90) を、必要に応じ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			て設定することができます。実際の値には、組織のポリシーを反映する必要があります。
8.2.4	ユーザーのパスワード/パスフレーズは、少なくとも90 日ごとに変更します。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.5	個人が過去に使用した 4 つのパスワード/パスフレーズと同じものを、新しいパスワード/パスフレーズとして送信することを許可しないでください。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、IAM パスワードポリシーの RequireUppercaseCharacters (PCI DSSデフォルト: false)、RequireLowercaseCharacters (PCI DSS デフォルト: true)、RequireSymbols (PCI DSS デフォルト: false)、RequireNumbers (PCI DSSデフォルト: true)、MinimumPasswordLength (PCI DSSデフォルト: 7)、PasswordReusePrevention (PCI DSSデフォルト: 4)、MaxPasswordAge (PCI DSS デフォルト: 90) を、必要に応じ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			て設定することができます。実際の値には、組織のポリシーを反映する必要があります。
8.3.1	管理者のアクセス権を持つ担当者の CDE に、コンソール以外のすべてのアクセスに対する多要素認証を組み込みます。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.1	管理者のアクセス権を持つ担当者の CDE に、コンソール以外のすべてのアクセスに対する多要素認証を組み込みます。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.1	管理者のアクセス権を持つ担当者の CDE に、コンソール以外のすべてのアクセスに対する多要素認証を組み込みます。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.1	管理者のアクセス権を持つ担当者の CDE に、コンソール以外のすべてのアクセスに対する多要素認証を組み込みます。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	エンティティのネットワークの外部から発信されるすべてのリモートネットワークアクセス (ユーザーと管理者の両方、およびサポートまたはメンテナンスのためのサードパーティーアクセスを含む) に多要素認証を組み込みます。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	エンティティのネットワークの外部から発信されるすべてのリモートネットワークアクセス (ユーザーと管理者の両方、およびサポートまたはメンテナンスのためのサードパーティーアクセスを含む) に多要素認証を組み込みます。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	エンティティのネットワークの外部から発信されるすべてのリモートネットワークアクセス (ユーザーと管理者の両方、およびサポートまたはメンテナンスのためのサードパーティーアクセスを含む) に多要素認証を組み込みます。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	エンティティのネットワークの外部から発信されるすべてのリモートネットワークアクセス (ユーザーと管理者の両方、およびサポートまたはメンテナンスのためのサードパーティーアクセスを含む) に多要素認証を組み込みます。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、ユーザー名とパスワードに 1 つの保護レイヤーを追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.1	監査証跡を実装して、システムコンポーネントへのすべてのアクセスを個々のユーザーにリンクします。	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。個々のすべてのユーザーによるカード所有者データへのアクセス	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。ルート権限または管理者権限を持つすべての個人が実行したアクション	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。ルート権限または管理者権限を持つすべての個人が実行したアクション	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
10.2.2	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。ルート権限または管理者権限を持つすべての個人が実行したアクション	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。ルート権限または管理者権限を持つすべての個人が実行したアクション	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。
10.2.2	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。ルート権限または管理者権限を持つすべての個人が実行したアクション	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。ルート権限または管理者権限を持つすべての個人が実行したアクション	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
10.2.2	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。ルート権限または管理者権限を持つすべての個人が実行したアクション	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。ルート権限または管理者権限を持つすべての個人が実行したアクション	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.3	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。すべての監査証跡へのアクセス	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.4	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。無効な論理アクセスの試行	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.5	すべてのシステムコンポーネントに対して自動監査証跡を実装し、以下のイベントを再構築します。識別および認証メカニズムの使用および変更 (新規アカウントの作成や特権の昇格を含む、ただしこれに限定されない)、およびすべての変更、追加、またはルート権限または管理者権限を持つアカウントへの削除	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.5	すべてのシステムコンポーネントに対して自動監査証跡を実装し、以下のイベントを再構築します。識別および認証メカニズムの使用および変更 (新規アカウントの作成や特権の昇格を含む、ただしこれに限定されない)、およびすべての変更、追加、またはルート権限または管理者権限を持つアカウントへの削除	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.5	すべてのシステムコンポーネントに対して自動監査証跡を実装し、以下のイベントを再構築します。識別および認証メカニズムの使用および変更 (新規アカウントの作成や特権の昇格を含む、ただしこれに限定されない)、およびすべての変更、追加、またはルート権限または管理者権限を持つアカウントへの削除	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
10.2.5	すべてのシステムコンポーネントに対して自動監査証跡を実装し、以下のイベントを再構築します。識別および認証メカニズムの使用および変更 (新規アカウントの作成や特権の昇格を含む、ただしこれに限定されない)、およびすべての変更、追加、またはルート権限または管理者権限を持つアカウントへの削除	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.5	すべてのシステムコンポーネントに対して自動監査証跡を実装し、以下のイベントを再構築します。識別および認証メカニズムの使用および変更 (新規アカウントの作成や特権の昇格を含む、ただしこれに限定されない)、およびすべての変更、追加、またはルート権限または管理者権限を持つアカウントへの削除	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
10.2.5	すべてのシステムコンポーネントに対して自動監査証跡を実装し、以下のイベントを再構築します。識別および認証メカニズムの使用および変更 (新規アカウントの作成や特権の昇格を含む、ただしこれに限定されない)、およびすべての変更、追加、またはルート権限または管理者権限を持つアカウントへの削除	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.5	すべてのシステムコンポーネントに対して自動監査証跡を実装し、以下のイベントを再構築します。識別および認証メカニズムの使用および変更 (新規アカウントの作成や特権の昇格を含む、ただしこれに限定されない)、およびすべての変更、追加、またはルート権限または管理者権限を持つアカウントへの削除	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.5	すべてのシステムコンポーネントに対して自動監査証跡を実装し、以下のイベントを再構築します。識別および認証メカニズムの使用および変更 (新規アカウントの作成や特権の昇格を含む、ただしこれに限定されない)、およびすべての変更、追加、またはルート権限または管理者権限を持つアカウントへの削除	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.6	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。監査ログの初期化、停止、または一時停止	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.6	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。監査ログの初期化、停止、または一時停止	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
10.2.6	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。監査ログの初期化、停止、または一時停止	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.7	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。システムレベルオブジェクトの作成と削除	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.7	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。システムレベルオブジェクトの作成と削除	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.7	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。システムレベルオブジェクトの作成と削除	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
10.2.7	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。システムレベルオブジェクトの作成と削除	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.7	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。システムレベルオブジェクトの作成と削除	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
10.2.7	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。システムレベルオブジェクトの作成と削除	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.7	すべてのシステムコンポーネントの自動監査証跡を実装して、以下のイベントを再構築します。システムレベルオブジェクトの作成と削除	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時刻、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	各イベントですべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録します: ユーザー ID	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5	監査証跡を改ざんできないように保護します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
10.5	監査証跡を改ざんできないように保護します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5	監査証跡を改ざんできないように保護します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
10.5.2	監査証跡ファイルを不正な変更から保護します。	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.2	監査証跡ファイルを不正な変更から保護します。	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
10.5.2	監査証跡ファイルを不正な変更から保護します。	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.3	変更が難しい一元管理されたログサーバーまたはメディアで、監査証跡ファイルをただちにバックアップします。	s3-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.3	変更が難しい一元管理されたログサーバーまたはメディアで、監査証跡ファイルをただちにバックアップします。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
10.5.3	変更が難しい一元管理されたログサーバーまたはメディアで、監査証跡ファイルをただちにバックアップします。	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
10.5.3	変更が難しい一元管理されたログサーバーまたはメディアで、監査証跡ファイルをただちにバックアップします。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.5	ログにファイル整合性モニタリングソフトウェアまたは変更検出ソフトウェアを使用して、アラートを生成しなくても既存のログデータが変更されないようにします(ただし、新しいデータを追加してもアラートは生成しません)。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.5	ログにファイル整合性モニタリングソフトウェアまたは変更検出ソフトウェアを使用して、アラートを生成しなくても既存のログデータが変更されないようにします(ただし、新しいデータを追加してもアラートは生成しません)。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7	監査証跡の履歴を少なくとも 1 年間保持し、最低 3 ヶ月はすぐに分析できるようにする (例: オンライン、アーカイブ、またはバックアップから復元可能)。	s3-lifecycle-policy-check	Amazon S3 のライフサイクルポリシーが、オブジェクトのライフタイム中に Amazon S3 が実行するアクションの定義に役立つように設定されていることを確認します (他のストレージクラスへのオブジェクトの移行や指定した期間後のオブジェクトのアーカイブや削除など)。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7	監査証跡の履歴を少なくとも 1 年間保持し、最低 3 ヶ月はすぐに分析できるようにする (例: オンライン、アーカイブ、またはバックアップから復元可能)。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
11.2.3	内部スキャンと外部スキャンを実行し、大幅な変更があった場合は必要に応じて再スキャンします。スキャンは資格のある担当者が実行する必要があります。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを有効にすると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	侵入検知/防御テクノロジーを使用して、ネットワークへの侵入を検知、防止します。カード会員データ環境の境界およびカード会員データ環境の重要なポイントにおけるすべてのトラフィックを監視し、危殆化の疑いがある場合は担当者に警告します。すべての侵入検知や防止エンジン、ベースライン、シグネチャを常に最新の状態に保ちます。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.4	侵入検知/防御テクノロジーを使用して、ネットワークへの侵入を検知、防止します。カード会員データ環境の境界およびカード会員データ環境の重要なポイントにおけるすべてのトラフィックを監視し、危殆化の疑いがある場合は担当者に警告します。すべての侵入検知や防止エンジン、ベースライン、シグネチャを常に最新の状態に保ちます。	netfw-policy-rule-group-associated	AWS Network Firewall ポリシーは、ファイアウォールが Amazon VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定して、パケットとトラフィックフローのフィルタリングし、デフォルトのトラフィック処理を定義します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.5	重要なシステムファイル、設定ファイル、コンテンツファイルの不正な変更 (変更、追加、削除を含む) を担当者に警告するための変更検出メカニズム (例: ファイル整合性監視ツール) を導入し、少なくとも週に一度は重要ファイルの比較を実行するようにソフトウェアを構成します。	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.5	重要なシステムファイル、設定ファイル、コンテンツファイルの不正な変更 (変更、追加、削除を含む) を担当者に警告するための変更検出メカニズム (例: ファイル整合性監視ツール) を導入し、少なくとも週に一度は重要ファイルの比較を実行するようにソフトウェアを構成します。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for PCI DSS 3.2.1」で入手できます。

PCI DSS 4.0 の運用上のベストプラクティス (グローバルリソースタイプを除く)

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成

できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Payment Card Industry Data Security Standard (PCI DSS) 4.0 (グローバルリソースタイプを除く) と AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の PCI DSS コントロールに関連付けられます。「PCI DSS」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.5	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	transfer-family-server-no-ftp	AWS Transfer Family で作成されたサーバーがエンドポイント接続に FTP を使用しないようにしてください。エンドポイント接続のサーバープロトコルが FTP 対応の場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルール

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			は NON_COMPLIANT を返します。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントへの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントへの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントへの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.1	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
1.4.1	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.1	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントへの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.3	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.3	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。
1.4.3	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	netfw-policy-default-action-full-packets	AWS Network Firewall ポリシーが、フルパケットに対してユーザー定義のデフォルトのステートレスアクションで設定されていることを確認します。完全なパケットのデフォルトステートレスアクションがユーザー定義のデフォルトステートレスアクションと一致しない場合、このルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.4	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
1.4.4	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.4	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。
1.4.5	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	ecs-task-definition-pid-mode-check	ECSTaskDefinitions が、ホストのプロセス名前空間をその Amazon Elastic Container Service (Amazon ECS) コンテナと共有するように設定されてことを確認します。pidMode パラメータが「host」に設定されている場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.5	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	ec2-launch-template-public-ip-disabled	Amazon EC2 起動テンプレートが、ネットワークインターフェイスにパブリック IP アドレスを割り当てるように設定されていることを確認します。EC2 起動テンプレートのデフォルトバージョンで、「AssociatePublicIpAddress」が「true」に設定されているネットワークが 1 つまたは複数ある場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントへの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 手動 DB クラスタースナップショットがパブリックでないことを確認します。既存および新規の Neptune スナップショットがパブリックの場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	バックアップ計画によって保護された aurora リソース	Amazon Aurora DB クラスターがバックアッププランで保護されていることを確認します。Amazon Relational Database Service (Amazon RDS) データベースクラスターがバックアッププランによって保護されていない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	db-instance-backup-enabled	RDS DB インスタンスでバックアップが有効になっていることを確認します。オプションで、バックアップ保存期間およびバックアップウィンドウを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	dynamodb-in-backup-plan	Amazon DynamoDB テーブルが AWS Backup Plans に存在することを確認します。Amazon DynamoDB テーブルが AWS Backup プランに存在しない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	dynamodb-バックアップ計画によって保護されるリソース	Amazon DynamoDB テーブルがバックアップ計画で保護されていることを確認します。DynamoDB テーブルがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	ebs-in-backup-plan	Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup のバックアッププランに追加されていることを確認します。Amazon EBS ボリュームが Backup プランに含まれていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	バックアップ計画によって保護されたEBS リソース	Amazon Elastic Block Store (Amazon EBS) ボリュームが、バックアップ計画に追加されていることを確認します。Amazon EBSボリュームがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	EC2-バックアップ計画によって保護されるリソース	Amazon Elastic Compute Cloud (Amazon EC2) インスタンスがバックアップ計画で保護されていることを確認します。Amazon EC2 インスタンスがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	バックアップ計画によって保護された efs リソース	Amazon Elastic File System (Amazon EFS) ファイルシステムがバックアップ計画で保護されていることを確認します。EFS ファイルがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	elasticache-redis-cluster-automatic-backup-check	Amazon ElastiCache Redis クラスターで自動バックアップが有効になっているかどうかを確認します。Redis クラスターの SnapshotRetentionLimit が SnapshotRetentionPeriod パラメータより小さい場合、ルールは NON_COMPLIANT です。例えば、パラメータが 15 の場合、snapshotRetentionPeriod が 0 ~ 15 であれば、ルールは準拠していません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	fsx-リソース-バックアップ計画によって保護される	Amazon FSx ファイルシステムがバックアップ計画で保護されていることを確認します。Amazon FSx ファイルがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	neptune-cluster-backup-retention-check	Amazon Neptune DB クラスターの保持期間が特定の日数に設定されていることを確認します。保持期間がパラメータで指定された値よりも短い場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	rds-in-backup-plan	Amazon Relational Database Service (Amazon RDS) データベースが AWS Backup プランに存在することを確認します。Amazon RDS データベースが AWS Backup プランに含まれていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	redshift-backup-enabled	Amazon Redshift 自動スナップショットがクラスターに対して有効になっていることを確認します。automatedSnapshotRetentionPeriod の値が MaxRetentionPeriod より大きいか MinRetentionPeriod より小さいか、値が 0 である場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-resources-protected-by-backup-plan	Amazon Simple Storage Service (Amazon S3) バケットがバックアッププランで保護されていることを確認します。Amazon S3 バケットがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	db-instance-backup-enabled	RDS DB インスタンスでバックアップが有効になっていることを確認します。オプションで、バックアップ保存期間およびバックアップウィンドウを確認します。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.4	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-bucket-default-lock-enabled	デフォルトでは、S3 バケットのロックが有効になっていることを確認します。ロックが有効でない場合、ルールは NON_COMPLIANT です。
10.3.4	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-bucket-versioning-enabled	S3 バケットでバージョニングが有効になっていることを確認します。オプションで、S3 バケットに対して MFA 削除が有効になっているかどうかを確認します。
10.3.4	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.4.3	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
11.5.2	ネットワーク侵入と予期しないファイル変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.5.2	ネットワーク侵入と予期しないファイル変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。
11.5.2	ネットワーク侵入と予期しないファイル変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.5.2	ネットワーク侵入と予期しないファイル変更は、検出および応答されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
11.6.1	支払いページの不正な変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.6.1	支払いページの不正な変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。
11.6.1	支払いページの不正な変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.6.1	支払いページの不正な変更は、検出および応答されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
12.10.5	CDE に影響を与える可能性のあるセキュリティインシデントが疑われ、確認された場合は、すぐに応答します。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.10.5	CDE に影響を与える可能性のあるセキュリティインシデントが疑われ、確認された場合は、すぐに応答します。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。
12.10.5	CDE に影響を与える可能性のあるセキュリティインシデントが疑われ、確認された場合は、すぐに応答します。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.10.5	CDE に影響を与える可能性のあるセキュリティインシデントが疑われ、確認された場合は、すぐに応答します。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
12.4.2.1	PCI DSS コンプライアンスは管理されています。(PCI-DSS-v4.0)	service-catalog-shared-within-organization	Organizations との統合が有効になっている場合は、 AWS Service Catalog がポートフォリオを組織 (単一ユニットとして扱われる AWS アカウントのコレクション) AWS と共有していることを確認します。共有の「Type」値が「ACCOUNT」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.5	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	transfer-family-server-no-ftp	AWS Transfer Family で作成されたサーバーがエンドポイント接続に FTP を使用しないようにしてください。エンドポイント接続のサーバープロトコルが FTP 対応の場合、ルールは NON_COMPLIANT です。
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、他のエンドポイントと通信されるデータの TLS/SSL 暗号化が有効になっていることを確認します。TLS/SSL が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) を使用して転送中に暗号化を適用していることを確認します。プレーンテキスト通信がクラスター内ブローカーノード接続に対して有効になっている場合、ルールは NON_COMPLIANT です。
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service (AWS DMS) エンドポイントが SSL 接続で設定されていることを確認します。DMS に SSL AWS 接続が設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1	アカウントデータの保存は最小限に抑えられます。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.2.1	アカウントデータの保存は最小限に抑えられます。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1	アカウントデータの保存は最小限に抑えられます。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.2.1	アカウントデータの保存は最小限に抑えられます。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1.1	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.3.1.1	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1.1	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.3.1.1	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.3.1.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.3.1.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.3.2	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.3.2	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.3.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.3.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	athena-workgroup-encrypted-at-rest	Amazon Athena ワークグループが保管中に暗号化されていることを確認します。Athena ワークグループで保管中のデータの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Amazon Neptune DB クラスターのスナップショットが暗号化されていることを確認します。Neptune クラスターのスナップショットが暗号化されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Amazon Redshift クラスターが、暗号化に指定された AWS Key Management Service (AWS KMS) キーを使用していることを確認します。暗号化が有効になっていて、クラスターが kmsKeyArn パラメータで指定されたキーで暗号化されている場合、ルールは COMPLIANT です。クラスターが暗号化されていない場合、または別のキーで暗号化されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	codebuild-project-s3-logs-encrypted	Amazon S3 Logs で設定された an AWS CodeBuild プロジェクトで、ログに対して暗号化が有効になっていることを確認します。CodeBuild プロジェクトの S3LogsConfig で「encryptionDisabled」が「true」に設定されている場合、ルールは NON_COMPLIANT になります。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	eks-secrets-encrypted	Amazon Elastic Kubernetes Service クラスターが、 AWS Key Management Service (KMS) キーを使用して Kubernetes シークレットを暗号化するように設定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	api-gw-cache-enabled-and-encrypted	Amazon API Gateway ステージのすべてのメソッドでキャッシュが有効になっているか、および暗号化されていることを確認します。Amazon API Gateway ステージのいずれかのメソッドでキャッシュが設定されていない場合、またはキャッシュが暗号化されていない場合、ルールは NON_COMPLIANT です。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルが AWS Key Management Service (KMS) で暗号化されていることを確認します。Amazon DynamoDB テーブルが KMS で暗号化されていない場合、ルールは NON_COMPLIANT AWS です。暗号化された KMS キーが kmsKeyArns AWS 入力パラメータに存在しない場合も、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	環境変数 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY がプロジェクトに含まていないことを確認します。プロジェクト環境変数にプレーンテキストの認証情報が含まれている場合、ルールは NON_COMPLIANT です。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Amazon EKS クラスターが AWS KMS を使用して Kubernetes シークレットを暗号化するように設定されていないことを確認します。EKS クラスターに encryptionConfig リソースがない場合、または encryptionConfig がシークレットにリソースとして命名していない場合、このルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	kinesis-stream-encrypted	Amazon Kinesis Streams がサーバー側の暗号化を使用して保存時に暗号化されていることを確認します。「StreamEncryption」が存在しない場合、ルールは Kinesis ストリームに対して NON_COMPLIANT になります。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	neptune-cluster-encrypted	Amazon Neptune DB クラスターでストレージ暗号化が有効になっていることを確認します。ストレージの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。
3.5.1.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 手動 DB クラスタースナップショットがパブリックでないことを確認します。既存および新規の Neptune スナップショットがパブリックの場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
3.6.1	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1.2	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
3.6.1.2	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1.3	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
3.6.1.3	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1.4	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
3.6.1.4	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.1	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-certificate-rsa-check	AWS Certificate Manager (ACM) によって管理される RSA 証明書のキー長が少なくとも '2048' ビットであることを確認します。最小キー長が 2048 ビット未満の場合、ルールは NON_COMPLIANT です。
3.7.1	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.1	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
3.7.2	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.2	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
3.7.4	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.4	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
3.7.6	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.6	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
3.7.7	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.7	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、他のエンドポイントと通信されるデータの TLS/SSL 暗号化が有効になっていることを確認します。TLS/SSL が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) を使用して転送中に暗号化を適用していることを確認します。プレーンテキスト通信がクラスター内ブローカーノード接続に対して有効になっている場合、ルールは NON_COMPLIANT です。
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service (AWS DMS) エンドポイントが SSL 接続で設定されていることを確認します。DMS に SSL AWS 接続が設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、他のエンドポイントと通信されるデータの TLS/SSL 暗号化が有効になっていることを確認します。TLS/SSL が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) を使用して転送中に暗号化を適用していることを確認します。プレーンテキスト通信がクラスター内ブローカーノード接続に対して有効になっている場合、ルールは NON_COMPLIANT です。
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service (AWS DMS) エンドポイントが SSL 接続で設定されていることを確認します。DMS に SSL AWS 接続が設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。
6.3.3	セキュリティの脆弱性を特定し、対処します。(PCI-DSS-v4.0)	lambda-function-settings-check	ランタイム、ロール、タイムアウト、メモリサイズの AWS Lambda 関数設定が、想定値と一致していることを確認します。このルールは、「Image」パッケージタイプの関数と、「OS 専用ランタイム」に設定されたランタイムの関数を無視します。Lambda 関数の設定が期待値と一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3.3	セキュリティの脆弱性を特定し、対処します。(PCI-DSS-v4.0)	eks-cluster-oldest-supported-version	Amazon Elastic Kubernetes Service (EKS) クラスターが、サポートされているバージョンで最も古いものを実行していることを確認します。EKS クラスターがサポートされている最も古いバージョンを実行している場合 (パラメータ 「oldestVersionSupported」に等しい)、ルールは NON_COMPLIANT になります。
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	wafv2-webacl-not-empty	WAFv2 ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていない場合、ルールは NON_COMPLIANT です。
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	wafv2-rulegroup-not-empty	WAFv2 ルールグループにルールが含まれていることを確認します。WAFv2 ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	wafv2-webacl-not-empty	WAFv2 ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていない場合、ルールは NON_COMPLIANT です。
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	wafv2-rulegroup-not-empty	WAFv2 ルールグループにルールが含まれていることを確認します。WAFv2 ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
6.5.5	すべてのシステムコンポーネントへの変更は安全に管理されます。(PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-disabled	Lambda コンピューティングプラットフォームのデプロイグループがデフォルトのデプロイ設定を使用していることを確認します。デプロイグループが「CodeDeployDefault.LambdaAllAtOnce」のデプロイ設定を使用している場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.5.6	すべてのシステムコンポーネントへの変更は安全に管理されます。(PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-disabled	Lambda コンピューティングプラットフォームのデプロイグループがデフォルトのデプロイ設定を使用していることを確認します。デプロイグループが「CodeDeployDefault.LambdaAllAtOnce」のデプロイ設定を使用している場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.4	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	Secrets Manager シーAWS クレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	Secrets Manager シークレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.6	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.6	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。
8.2.1	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	環境変数 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY がプロジェクトに含まていないことを確認します。プロジェクト環境変数にプレーンテキストの認証情報が含まれている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	Secrets Manager シークレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.2.4	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.4	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.2.5	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.5	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.2.6	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	Secrets Manager シークレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-imdsv2-check	Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのメタデータのバージョンが、Instance Metadata Service Version 2 (IMDSv2) で設定されていることを確認します。HttpTokens が「optional」に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	autoscaling-launchconfig-requires-imdsv2	IMDSv2 のみが有効になっていることを確認します。メタデータのバージョンが起動設定に含まれていない場合、またはメタデータ V1 と V2 の両方が有効になっている場合、このルールは非準拠です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.10.1	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.3.10.1	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.10.1	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.3.11	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.11	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	athena-workgroup-encrypted-at-rest	Amazon Athena ワークグループが保管中に暗号化されていることを確認します。Athena ワークグループで保管中のデータの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Amazon Neptune DB クラスターのスナップショットが暗号化されていることを確認します。Neptune クラスターのスナップショットが暗号化されていない場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Amazon Redshift クラスターが、暗号化に指定された AWS Key Management Service (AWS KMS) キーを使用していることを確認します。暗号化が有効になっていて、クラスターが kmsKeyArn パラメータで指定されたキーで暗号化されている場合、ルールは COMPLIANT です。クラスターが暗号化されていない場合、または別のキーで暗号化されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	codebuild-project-s3-logs-encrypted	Amazon S3 Logs で設定された an AWS CodeBuild プロジェクトで、ログに対して暗号化が有効になっていることを確認します。CodeBuild プロジェクトの S3LogsConfig で「encryptionDisabled」が「true」に設定されている場合、ルールは NON_COMPLIANT になります。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、他のエンドポイントと通信されるデータの TLS/SSL 暗号化が有効になっていることを確認します。TLS/SSL が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	eks-secrets-encrypted	Amazon Elastic Kubernetes Service クラスターが、 AWS Key Management Service (KMS) キーを使用して Kubernetes シークレットを暗号化するように設定されていることを確認します。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	api-gw-cache-enabled-and-encrypted	Amazon API Gateway ステージのすべてのメソッドでキャッシュが有効になっているか、および暗号化されていることを確認します。Amazon API Gateway ステージのいずれかのメソッドでキャッシュが設定されていない場合、またはキャッシュが暗号化されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルが AWS Key Management Service (KMS) で暗号化されていることを確認します。Amazon DynamoDB テーブルが KMS で暗号化されていない場合、ルールは NON_COMPLIANT AWS です。暗号化された KMS キーが kmsKeyArns AWS 入力パラメータに存在しない場合も、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	環境変数 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY がプロジェクトに含まていないことを確認します。プロジェクト環境変数にプレーンテキストの認証情報が含まれている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Amazon EKS クラスターが AWS KMS を使用して Kubernetes シークレットを暗号化するように設定されていないことを確認します。EKS クラスターに encryptionConfig リソースがない場合、または encryptionConfig がシークレットにリソースとして命名していない場合、このルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	kinesis-stream-encrypted	Amazon Kinesis Streams がサーバー側の暗号化を使用して保存時に暗号化されていることを確認します。「StreamEncryption」が存在しない場合、ルールは Kinesis ストリームに対して NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) を使用して転送中に暗号化を適用していることを確認します。プレーンテキスト通信がクラスター内ブローカーノード接続に対して有効になっている場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	neptune-cluster-encrypted	Amazon Neptune DB クラスターでストレージ暗号化が有効になっていることを確認します。ストレージの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service (AWS DMS) エンドポイントが SSL 接続で設定されていることを確認します。DMS に SSL AWS 接続が設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.5	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.3.5	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.5	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.3.7	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.7	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。
8.3.7	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.9	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.3.9	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.9	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.4.1	CDE へのアクセスを保護するために、多要素認証 (MFA) が実装されています。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.4.2	CDE へのアクセスを保護するために、多要素認証 (MFA) が実装されています。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。
8.4.3	CDE へのアクセスを保護するために、多要素認証 (MFA) が実装されています。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.6.3	アプリケーションアカウントとシステムアカウント、および関連する認証要素の使用は厳しく管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.6.3	アプリケーションアカウントとシステムアカウント、および関連する認証要素の使用は厳しく管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.6.3	アプリケーションアカウントとシステムアカウント、および関連する認証要素の使用は厳しく管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 手動 DB クラスタースナップショットがパブリックでないことを確認します。既存および新規の Neptune スナップショットがパブリックの場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントへの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.3	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	security-account-information-provided	AWS アカウントの連絡先にセキュリティ連絡先情報を提供していることを確認します。アカウント内のセキュリティの連絡先情報が指定されていない場合、ルールは NON_COMPLIANT です。
A3.2.5.1	PCI DSS スコープは文書化され、検証されます。(PCI-DSS-v4.0)	macie-auto-sensitive-data-discovery-check	Amazon Macie で機密データの自動検出が有効になっていることを確認します。機密データの自動検出が無効になっている場合、ルールは NON_COMPLIANT です。このルールは管理者アカウントに適用され、メンバーアカウントには NOT_APPLICABLE です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.2.5.1	PCI DSS スコープは文書化され、検証されます。(PCI-DSS-v4.0)	macie-status-check	Amazon Macie がリージョンごとにアカウントで有効になっていることを確認します。「status」属性が「ENABLED」に設定されていない場合、ルールは NON_COMPLIANT です。
A3.2.5.2	PCI DSS スコープは文書化され、検証されます。(PCI-DSS-v4.0)	macie-auto-sensitive-data-discovery-check	Amazon Macie で機密データの自動検出が有効になっていることを確認します。機密データの自動検出が無効になっている場合、ルールは NON_COMPLIANT です。このルールは管理者アカウントに適用され、メンバーアカウントには NOT_APPLICABLE です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.2.5.2	PCI DSS スコープは文書化され、検証されます。(PCI-DSS-v4.0)	macie-status-check	Amazon Macie がリージョンごとにアカウントで有効になっていることを確認します。「status」属性が「ENABLED」に設定されていない場合、ルールは NON_COMPLIANT です。
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 手動 DB クラスタースナップショットがパブリックでないことを確認します。既存および新規の Neptune スナップショットがパブリックの場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	AWS Secrets Manager シークレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for PCI DSS 4.0 (グローバルリソースタイプを除く)」で入手できます。

PCI DSS 4.0 の運用上のベストプラクティス (グローバルリソースタイプを含む)

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、Payment Card Industry Data Security Standard (PCI DSS) 4.0 (グローバルリソースタイプを除く) と AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の PCI DSS コントロールに関連付けられます。「PCI DSS」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.5	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	cloudfront-security-policy-check	Amazon CloudFront ディストリビューションが、ビューワー接続に必要な最低限のセキュリティポリシーと、TLSv1.2 以上の暗号スイートを使用していることを確認します。minimumProtocolVersion が TLSv1.2_2018 より古い場合、CloudFront ディストリビューションでは、このルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.5	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	cloudfront-sni-enabled	Amazon CloudFront ディストリビューションでカスタム SSL 証明書が使用されていて、SNI を使用して HTTPS リクエストを処理するように設定されていることを確認します。カスタム SSL 証明書が関連付けられているものの、SSL サポートメソッドが専用 IP アドレスである場合、ルールは NON_COMPLIANT です。
1.2.5	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	transfer-family-server-no-ftp	AWS Transfer Family で作成されたサーバーがエンドポイント接続に FTP を使用しないようにしてください。エンドポイント接続のサーバープロトコルが FTP 対応の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.5	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront ディストリビューションが CloudFront エッジロケーションとカスタムオリジン間の HTTPS 通信に非推奨の SSL プロトコルを使用していないことを確認します。「OriginSslProtocols」に「SSLv3」が含まれる場合、このルールは CloudFront ディストリビューションで NON_COMPLIANT です。
1.2.5	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront ディストリビューションがカスタムオリジンへのトラフィックを暗号化していることを確認します。「OriginProtocolPolicy」が「http-only」、または「OriginProtocolPolicy」が「match-viewer」、かつ「ViewerProtocolPolicy」が「allow-all」である場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.5	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront ディストリビューションが HTTPS を (直接またはリダイレクト経由で) 使用していることを確認します。ViewerProtocolPolicy の値が DefaultCacheBehavior または CacheBehaviors に対して「allow-all」に設定されている場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront ディストリビューションがウェブアプリケーションファイアウォール (WAF) または WAFv2 ウェブアクセスコントロールリスト (ACL) に関連付けられていることを確認します。CloudFront ディストリビューションが WAF ウェブ ACL に関連付けられていない場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service (Amazon RDS) DB セキュリティグループがデフォルトであることを確認します。デフォルトの DB セキュリティグループではない DB セキュリティグループが存在する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud (Amazon EC2) トランジットゲートウェイで「AutoAcceptSharedAttachments」が有効になっていることを確認します。「AutoAcceptSharedAttachments」が「有効」に設定されている場合、ルールは、トランジットゲートウェイに対して NON_COMPLIANT になります。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、ルールは NON_COMPLIANT になります。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF グローバルルールにいくつかの条件が含まれていることを確認します。WAF グローバルルール内に条件がない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.2.8	ネットワークセキュリティコントロール (NSC) が設定され、維持されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront ディストリビューションがウェブアプリケーションファイアウォール (WAF) または WAFv2 ウェブアクセスコントロールリスト (ACL) に関連付けられていることを確認します。CloudFront ディストリビューションが WAF ウェブ ACL に関連付けられていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service (Amazon RDS) DB セキュリティグループがデフォルトであることを確認します。デフォルトの DB セキュリティグループではない DB セキュリティグループが存在する場合、ルールは NON_COMPLIANT になります。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud (Amazon EC2) トランジットゲートウェイで「AutoAcceptSharedAttachments」が有効になっていることを確認します。「AutoAcceptSharedAttachments」が「有効」に設定されている場合、ルールは、トランジットゲートウェイに対して NON_COMPLIANT になります。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、ルールは NON_COMPLIANT になります。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF グローバルルールにいくつかの条件が含まれていることを確認します。WAF グローバルルール内に条件がない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.3.1	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront ディストリビューションがウェブアプリケーションファイアウォール (WAF) または WAFv2 ウェブアクセスコントロールリスト (ACL) に関連付けられていることを確認します。CloudFront ディストリビューションが WAF ウェブ ACL に関連付けられていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service (Amazon RDS) DB セキュリティグループがデフォルトであることを確認します。デフォルトの DB セキュリティグループではない DB セキュリティグループが存在する場合、ルールは NON_COMPLIANT になります。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud (Amazon EC2) トランジットゲートウェイで「AutoAcceptSharedAttachments」が有効になっていることを確認します。「AutoAcceptSharedAttachments」が「有効」に設定されている場合、ルールは、トランジットゲートウェイに対して NON_COMPLIANT になります。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、ルールは NON_COMPLIANT になります。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF グローバルルールにいくつかの条件が含まれていることを確認します。WAF グローバルルール内に条件がない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.3.2	カード所有者データ環境とのネットワークアクセスは制限されています。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.1	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
1.4.1	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.1	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront ディストリビューションがウェブアプリケーションファイアウォール (WAF) または WAFv2 ウェブアクセスコントロールリスト (ACL) に関連付けられていることを確認します。CloudFront ディストリビューションが WAF ウェブ ACL に関連付けられていない場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service (Amazon RDS) DB セキュリティグループがデフォルトであることを確認します。デフォルトの DB セキュリティグループではない DB セキュリティグループが存在する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud (Amazon EC2) トランジットゲートウェイで「AutoAcceptSharedAttachments」が有効になっていることを確認します。「AutoAcceptSharedAttachments」が「有効」に設定されている場合、ルールは、トランジットゲートウェイに対して NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、ルールは NON_COMPLIANT になります。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF グローバルルールにいくつかの条件が含まれていることを確認します。WAF グローバルルール内に条件がない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.4.2	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.3	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.3	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。
1.4.3	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	netfw-policy-default-action-full-packets	AWS Network Firewall ポリシーに、フルパケットに対するユーザー定義のデフォルトのステートレスアクションが設定されていることを確認します。完全なパケットのデフォルトステートレスアクションがユーザー定義のデフォルトステートレスアクションと一致しない場合、このルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.4	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
1.4.4	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift クラスターで「enhancedVpcRouting」が有効になっていることを確認します。「enhancedVpcRouting」が有効でない場合、または configuration.enhancedVpcRouting フィールドが「false」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.4	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。
1.4.5	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	ecs-task-definition-pid-mode-check	ECSTaskDefinitions が、ホストのプロセス名前空間をその Amazon Elastic Container Service (Amazon ECS) コンテナと共有するように設定されてことを確認します。pidMode パラメータが「host」に設定されている場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.4.5	信頼されたネットワークと信頼されていないネットワーク間のネットワーク接続は制御されます。(PCI-DSS-v4.0)	ec2-launch-template-public-ip-disabled	Amazon EC2 起動テンプレートが、ネットワークインターフェイスにパブリック IP アドレスを割り当てるように設定されていることを確認します。EC2 起動テンプレートのデフォルトバージョンで、「AssociatePublicIpAddress」が「true」に設定されているネットワークが 1 つまたは複数ある場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront ディストリビューションがウェブアプリケーションファイアウォール (WAF) または WAFv2 ウェブアクセスコントロールリスト (ACL) に関連付けられていることを確認します。CloudFront ディストリビューションが WAF ウェブ ACL に関連付けられていない場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service (Amazon RDS) DB セキュリティグループがデフォルトであることを確認します。デフォルトの DB セキュリティグループではない DB セキュリティグループが存在する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud (Amazon EC2) トランジットゲートウェイで「AutoAcceptSharedAttachments」が有効になっていることを確認します。「AutoAcceptSharedAttachments」が「有効」に設定されている場合、ルールは、トランジットゲートウェイに対して NON_COMPLIANT になります。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、ルールは NON_COMPLIANT になります。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF グローバルルールにいくつかの条件が含まれていることを確認します。WAF グローバルルール内に条件がない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
1.5.1	信頼できないネットワークと CDE の両方に接続できるコンピューティングデバイスによる CDE へのリスクは軽減されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.1	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.3	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.4	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.5	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.6	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.1.7	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.2.2	監査ログは、異常や疑わしいアクティビティの検出、およびイベントのフォレンジック分析をサポートするために実装されます。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.1	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 手動 DB クラスタースナップショットがパブリックでないことを確認します。既存および新規の Neptune スナップショットがパブリックの場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。
10.3.2	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	バックアップ計画によって保護された aurora リソース	Amazon Aurora DB クラスターがバックアッププランで保護されていることを確認します。Amazon Relational Database Service (Amazon RDS) データベースクラスターがバックアッププランによって保護されていない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	db-instance-backup-enabled	RDS DB インスタンスでバックアップが有効になっていることを確認します。オプションで、バックアップ保存期間およびバックアップウィンドウを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	dynamodb-in-backup-plan	Amazon DynamoDB テーブルが AWS Backup Plans に存在することを確認します。Amazon DynamoDB テーブルが AWS Backup プランに存在しない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	dynamodb-バックアップ計画によって保護されるリソース	Amazon DynamoDB テーブルがバックアップ計画で保護されていることを確認します。DynamoDB テーブルがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	ebs-in-backup-plan	Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup のバックアッププランに追加されていることを確認します。Amazon EBS ボリュームが Backup プランに含まれていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	バックアップ計画によって保護されたEBS リソース	Amazon Elastic Block Store (Amazon EBS) ボリュームが、バックアップ計画に追加されていることを確認します。Amazon EBSボリュームがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	EC2-バックアップ計画によって保護されるリソース	Amazon Elastic Compute Cloud (Amazon EC2) インスタンスがバックアップ計画で保護されていることを確認します。Amazon EC2 インスタンスがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	efs-in-backup-plan	Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup のバックアッププランに追加されていることを確認します。EFS ファイルシステムがバックアッププランに含まれていない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	バックアップ計画によって保護された efs リソース	Amazon Elastic File System (Amazon EFS) ファイルシステムがバックアップ計画で保護されていることを確認します。EFS ファイルがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	elasticache-redis-cluster-automatic-backup-check	Amazon ElastiCache Redis クラスターで自動バックアップが有効になっているかどうかを確認します。Redis クラスターの SnapshotRetentionLimit が SnapshotRetentionPeriod パラメータより小さい場合、ルールは NON_COMPLIANT です。例えば、パラメータが 15 の場合、snapshotRetentionPeriod が 0 ~ 15 であれば、ルールは準拠していません。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	fsx-リソース-バックアップ計画によって保護される	Amazon FSx ファイルシステムがバックアップ計画で保護されていることを確認します。Amazon FSx ファイルがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	neptune-cluster-backup-retention-check	Amazon Neptune DB クラスターの保持期間が特定の日数に設定されていることを確認します。保持期間がパラメータで指定された値よりも短い場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	rds-in-backup-plan	Amazon Relational Database Service (Amazon RDS) データベースが AWS Backup プランに存在することを確認します。Amazon RDS データベースが AWS Backup プランに含まれていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	rds-バックアップ計画によって保護されるリソース	Amazon Relational Database Service (Amazon RDS) インスタンスがバックアップ計画で保護されていることを確認します。Amazon RDS データベースインスタンスがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	redshift-backup-enabled	Amazon Redshift 自動スナップショットがクラスターに対して有効になっていることを確認します。automatedSnapshotRetentionPeriod の値が MaxRetentionPeriod より大きいか MinRetentionPeriod より小さいか、値が 0 である場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-resources-protected-by-backup-plan	Amazon Simple Storage Service (Amazon S3) バケットがバックアッププランで保護されていることを確認します。Amazon S3 バケットがバックアップ計画の対象でない場合、ルールは NON_COMPLIANT です。
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	db-instance-backup-enabled	RDS DB インスタンスでバックアップが有効になっていることを確認します。オプションで、バックアップ保存期間およびバックアップウィンドウを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.3	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
10.3.4	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudfront-origin-access-identity-enabled	S3 オリジンタイプの CloudFront ディストリビューションにオリジンアクセスアイデンティティ (OAI) が設定されていることを確認します。CloudFront ディストリビューションが S3 によってバックアップされていて、オリジンタイプが OAI に設定されていない場合、またはオリジンが S3 バケットでない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.4	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudfront-s3-origin-access-control-enabled	Amazon Simple Storage Service (Amazon S3) オリジンタイプを使用する Amazon CloudFront ディストリビューションで、オリジンアクセスコントロール (OAC) が有効であることをチェックします。OAC が有効になっていない Amazon S3 オリジンを使用する CloudFront ディストリビューションの場合、ルールは NON_COMPLIANT になります。
10.3.4	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-bucket-default-lock-enabled	デフォルトでは、S3 バケットのロックが有効になっていることを確認します。ロックが有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.3.4	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	s3-bucket-versioning-enabled	S3 バケットでバージョニングが有効になっていることを確認します。オプションで、S3 バケットに対して MFA 削除が有効になっているかどうかを確認します。
10.3.4	監査ログは、破壊や不正な変更から保護されています。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.1.1	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.4.2	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.4.3	監査ログは、異常や疑わしいアクティビティを特定するためにレビューされます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.5.1	監査ログ履歴は保持され、分析に使用できます。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.6.3	時間同期メカニズムでは、すべてのシステムに一貫した時間設定をサポートします。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation スタックが Amazon SNS トピックにイベント通知を送信していることを確認します。オプションで、指定された Amazon SNS トピックが使用されていることを確認します。CloudFormation スタックが通知を送信しない場合、ルールは NON_COMPLIANT です。
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.1	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation スタックが Amazon SNS トピックにイベント通知を送信していることを確認します。オプションで、指定された Amazon SNS トピックが使用されていることを確認します。CloudFormation スタックが通知を送信しない場合、ルールは NON_COMPLIANT です。
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
10.7.2	重要なセキュリティコントロールシステムの障害は、迅速に検出、報告、対応されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
11.5.2	ネットワーク侵入と予期しないファイル変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation スタックが Amazon SNS トピックにイベント通知を送信していることを確認します。オプションで、指定された Amazon SNS トピックが使用されていることを確認します。CloudFormation スタックが通知を送信しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.5.2	ネットワーク侵入と予期しないファイル変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.5.2	ネットワーク侵入と予期しないファイル変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。
11.5.2	ネットワーク侵入と予期しないファイル変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.5.2	ネットワーク侵入と予期しないファイル変更は、検出および応答されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
11.6.1	支払いページの不正な変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation スタックが Amazon SNS トピックにイベント通知を送信していることを確認します。オプションで、指定された Amazon SNS トピックが使用されていることを確認します。CloudFormation スタックが通知を送信しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.6.1	支払いページの不正な変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.6.1	支払いページの不正な変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。
11.6.1	支払いページの不正な変更は、検出および応答されます。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
11.6.1	支払いページの不正な変更は、検出および応答されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
12.10.5	CDE に影響を与える可能性のあるセキュリティインシデントが疑われ、確認された場合は、すぐに応答します。(PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation スタックが Amazon SNS トピックにイベント通知を送信していることを確認します。オプションで、指定された Amazon SNS トピックが使用されていることを確認します。CloudFormation スタックが通知を送信しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.10.5	CDE に影響を与える可能性のあるセキュリティインシデントが疑われ、確認された場合は、すぐに応答します。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.10.5	CDE に影響を与える可能性のあるセキュリティインシデントが疑われ、確認された場合は、すぐに応答します。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。
12.10.5	CDE に影響を与える可能性のあるセキュリティインシデントが疑われ、確認された場合は、すぐに応答します。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
12.10.5	CDE に影響を与える可能性のあるセキュリティインシデントが疑われ、確認された場合は、すぐに応答します。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。
12.4.2.1	PCI DSS コンプライアンスは管理されています。(PCI-DSS-v4.0)	service-catalog-shared-within-organization	Organizations との統合が有効になっている場合は、 AWS Service Catalog がポートフォリオを組織 (単一ユニットとして扱われる AWS アカウントのコレクション) AWS と共有していることを確認します。共有の「Type」値が「ACCOUNT」の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.5	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	cloudfront-security-policy-check	Amazon CloudFront ディストリビューションが、ビューワー接続に必要な最低限のセキュリティポリシーと、TLSv1.2 以上の暗号スイートを使用していることを確認します。minimumProtocolVersion が TLSv1.2_2018 より古い場合、CloudFront ディストリビューションでは、このルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.5	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	cloudfront-sni-enabled	Amazon CloudFront ディストリビューションでカスタム SSL 証明書が使用されていて、SNI を使用して HTTPS リクエストを処理するように設定されていることを確認します。カスタム SSL 証明書が関連付けられているものの、SSL サポートメソッドが専用 IP アドレスである場合、ルールは NON_COMPLIANT です。
2.2.5	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	transfer-family-server-no-ftp	AWS Transfer Family で作成されたサーバーがエンドポイント接続に FTP を使用しないようにしてください。エンドポイント接続のサーバープロトコルが FTP 対応の場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.5	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront ディストリビューションが CloudFront エッジロケーションとカスタムオリジン間の HTTPS 通信に非推奨の SSL プロトコルを使用していないことを確認します。「OriginSslProtocols」に「SSLv3」が含まれる場合、このルールは CloudFront ディストリビューションで NON_COMPLIANT です。
2.2.5	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront ディストリビューションがカスタムオリジンへのトラフィックを暗号化していることを確認します。「OriginProtocolPolicy」が「http-only」、または「OriginProtocolPolicy」が「match-viewer」、かつ「ViewerProtocolPolicy」が「allow-all」である場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.5	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront ディストリビューションが HTTPS を (直接またはリダイレクト経由で) 使用していることを確認します。ViewerProtocolPolicy の値が DefaultCacheBehavior または CacheBehaviors に対して「allow-all」に設定されている場合、ルールは NON_COMPLIANT です。
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、他のエンドポイントと通信されるデータの TLS/SSL 暗号化が有効になっていることを確認します。TLS/SSL が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront ディストリビューションが CloudFront エッジロケーションとカスタムオリジン間の HTTPS 通信に非推奨の SSL プロトコルを使用していないことを確認します。「OriginSslProtocols」に「SSLv3」が含まれる場合、このルールは CloudFront ディストリビューションで NON_COMPLIANT です。
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront ディストリビューションがカスタムオリジンへのトラフィックを暗号化していることを確認します。「OriginProtocolPolicy」が「http-only」、または「OriginProtocolPolicy」が「match-viewer」、かつ「ViewerProtocolPolicy」が「allow-all」である場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront ディストリビューションが HTTPS を (直接またはリダイレクト経由で) 使用していることを確認します。ViewerProtocolPolicy の値が DefaultCacheBehavior または CacheBehaviors に対して「allow-all」に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Amazon DynamoDB Accelerator (DAX) クラスターの ClusterEndpointEncryptionType が TLS に設定されていることを確認します。DAX クラスターが Transport Layer Security (TLS) によって暗号化されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) を使用して転送中に暗号化を適用していることを確認します。プレーンテキスト通信がクラスター内ブローカーノード接続に対して有効になっている場合、ルールは NON_COMPLIANT です。
2.2.7	システムコンポーネントは安全に設定および管理されます。(PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service (AWS DMS) エンドポイントが SSL 接続で設定されていることを確認します。DMS に SSL AWS 接続が設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1	アカウントデータの保存は最小限に抑えられます。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.2.1	アカウントデータの保存は最小限に抑えられます。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.2.1	アカウントデータの保存は最小限に抑えられます。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.2.1	アカウントデータの保存は最小限に抑えられます。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1.1	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.3.1.1	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1.1	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.3.1.1	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.3.1.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.1.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.3.1.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.3.2	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.2	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.3.2	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS ボリュームが EC2 インスタンスにアタッチされていることを確認します。オプションで、インスタンスの削除時に EBS ボリュームが削除対象としてマークされることを確認します。
3.3.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	プライベート Amazon Elastic Container Registry (ECR) リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されていることを確認します。ECR プライベートリポジトリに対してライフサイクルポリシーが設定されていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	dynamodb-pitr-enabled	ポイントインタイムリカバリ (PITR) が Amazon DynamoDB テーブルに対して有効になっていることを確認します。PITR が DynamoDB テーブルに対して有効になっていない場合、ルールは NON_COMPLIANT です。
3.3.3	承認された機密認証データ (SAD) は保存されません。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	athena-workgroup-encrypted-at-rest	Amazon Athena ワークグループが保管中に暗号化されていることを確認します。Athena ワークグループで保管中のデータの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Amazon Neptune DB クラスターのスナップショットが暗号化されていることを確認します。Neptune クラスターのスナップショットが暗号化されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Amazon Redshift クラスターが、暗号化に指定された AWS Key Management Service (AWS KMS) キーを使用していることを確認します。暗号化が有効になっていて、クラスターが kmsKeyArn パラメータで指定されたキーで暗号化されている場合、ルールは COMPLIANT です。クラスターが暗号化されていない場合、または別のキーで暗号化されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	codebuild-project-artifact-encryption	an AWS CodeBuild プロジェクトで、すべてのアーティファクトに対して暗号化が有効になっていることを確認します。プライマリまたはセカンダリ (存在する場合) のアーティファクト設定のいずれかに「encryptionDisabled」が「true」に設定されていると、ルールは NON_COMPLIANT になります。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	codebuild-project-s3-logs-encrypted	Amazon S3 Logs で設定された an AWS CodeBuild プロジェクトで、ログに対して暗号化が有効になっていることを確認します。CodeBuild プロジェクトの S3LogsConfig で「encryptionDisabled」が「true」に設定されている場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	dax-encryption-enabled	Amazon DynamoDB Accelerator (DAX) クラスターが暗号化されていることを確認します。DAX クラスターが暗号化されていない場合、ルールは NON_COMPLIANT です。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	eks-secrets-encrypted	Amazon Elastic Kubernetes Service クラスターが、 AWS Key Management Service (KMS) キーを使用して Kubernetes シークレットを暗号化するように設定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	api-gw-cache-enabled-and-encrypted	Amazon API Gateway ステージのすべてのメソッドでキャッシュが有効になっているか、および暗号化されていることを確認します。Amazon API Gateway ステージのいずれかのメソッドでキャッシュが設定されていない場合、またはキャッシュが暗号化されていない場合、ルールは NON_COMPLIANT です。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	docdb-cluster-encrypted	Amazon DocumentDB (MongoDB 互換) クラスターでストレージ暗号化が有効になっていることを確認します。ストレージの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルが AWS Key Management Service (KMS) で暗号化されていることを確認します。Amazon DynamoDB テーブルが KMS で暗号化されていない場合、ルールは NON_COMPLIANT AWS です。暗号化された KMS キーが kmsKeyArns AWS 入力パラメータに存在しない場合も、ルールは NON_COMPLIANT です。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	dynamodb-table-encryption-enabled	Amazon DynamoDB テーブルが暗号化されていること、およびそのステータスを確認します。ステータスが有効または有効化中の場合、ルールは COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	環境変数 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY がプロジェクトに含まていないことを確認します。プロジェクト環境変数にプレーンテキストの認証情報が含まれている場合、ルールは NON_COMPLIANT です。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Amazon EKS クラスターが AWS KMS を使用して Kubernetes シークレットを暗号化するように設定されていないことを確認します。EKS クラスターに encryptionConfig リソースがない場合、または encryptionConfig がシークレットにリソースとして命名していない場合、このルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	kinesis-stream-encrypted	Amazon Kinesis Streams がサーバー側の暗号化を使用して保存時に暗号化されていることを確認します。「StreamEncryption」が存在しない場合、ルールは Kinesis ストリームに対して NON_COMPLIANT になります。
3.5.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	neptune-cluster-encrypted	Amazon Neptune DB クラスターでストレージ暗号化が有効になっていることを確認します。ストレージの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。
3.5.1.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
3.5.1.1	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 手動 DB クラスタースナップショットがパブリックでないことを確認します。既存および新規の Neptune スナップショットがパブリックの場合、ルールは NON_COMPLIANT です。
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。
3.5.1.3	プライマリアカウント番号 (PAN) は、保存場所にかかわらず保護されます。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
3.6.1	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
3.6.1.2	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1.2	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
3.6.1.2	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1.3	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
3.6.1.3	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1.3	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
3.6.1.4	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.6.1.4	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
3.6.1.4	保存されたアカウントデータの保護に使用される暗号化キーは保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.1	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-certificate-rsa-check	AWS Certificate Manager (ACM) によって管理される RSA 証明書のキー長が少なくとも '2048' ビットであることを確認します。最小キー長が 2048 ビット未満の場合、ルールは NON_COMPLIANT です。
3.7.1	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.1	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
3.7.1	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.2	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
3.7.2	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.2	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
3.7.4	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.4	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
3.7.4	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.6	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
3.7.6	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.6	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
3.7.7	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.7.7	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
3.7.7	暗号化を使用して保存されたアカウントデータを保護する場合、キーライフサイクルのすべての側面をカバーするキー管理プロセスと手順が定義および実装されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、他のエンドポイントと通信されるデータの TLS/SSL 暗号化が有効になっていることを確認します。TLS/SSL が有効でない場合、ルールは NON_COMPLIANT です。
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront ディストリビューションが CloudFront エッジロケーションとカスタムオリジン間の HTTPS 通信に非推奨の SSL プロトコルを使用していないことを確認します。「OriginSslProtocols」に「SSLv3」が含まれる場合、このルールは CloudFront ディストリビューションで NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront ディストリビューションがカスタムオリジンへのトラフィックを暗号化していることを確認します。「OriginProtocolPolicy」が「http-only」、または「OriginProtocolPolicy」が「match-viewer」、かつ「ViewerProtocolPolicy」が「allow-all」である場合、ルールは NON_COMPLIANT です。
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront ディストリビューションが HTTPS を (直接またはリダイレクト経由で) 使用していることを確認します。ViewerProtocolPolicy の値が DefaultCacheBehavior または CacheBehaviors に対して「allow-all」に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Amazon DynamoDB Accelerator (DAX) クラスターの ClusterEndpointEncryptionType が TLS に設定されていることを確認します。DAX クラスターが Transport Layer Security (TLS) によって暗号化されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) を使用して転送中に暗号化を適用していることを確認します。プレーンテキスト通信がクラスター内ブローカーノード接続に対して有効になっている場合、ルールは NON_COMPLIANT です。
4.2.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service (AWS DMS) エンドポイントが SSL 接続で設定されていることを確認します。DMS に SSL AWS 接続が設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	acm-pca-root-ca-disabled	Private Certificate Authority (AWS Private CA) AWS のルート CA が無効になっていることを確認します。ルールは、ルート CA の NON_COMPLIANT のステータスが DISABLED になっていないことです。
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、他のエンドポイントと通信されるデータの TLS/SSL 暗号化が有効になっていることを確認します。TLS/SSL が有効でない場合、ルールは NON_COMPLIANT です。
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront ディストリビューションが CloudFront エッジロケーションとカスタムオリジン間の HTTPS 通信に非推奨の SSL プロトコルを使用していないことを確認します。「OriginSslProtocols」に「SSLv3」が含まれる場合、このルールは CloudFront ディストリビューションで NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront ディストリビューションがカスタムオリジンへのトラフィックを暗号化していることを確認します。「OriginProtocolPolicy」が「http-only」、または「OriginProtocolPolicy」が「match-viewer」、かつ「ViewerProtocolPolicy」が「allow-all」である場合、ルールは NON_COMPLIANT です。
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront ディストリビューションが HTTPS を (直接またはリダイレクト経由で) 使用していることを確認します。ViewerProtocolPolicy の値が DefaultCacheBehavior または CacheBehaviors に対して「allow-all」に設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Amazon DynamoDB Accelerator (DAX) クラスターの ClusterEndpointEncryptionType が TLS に設定されていることを確認します。DAX クラスターが Transport Layer Security (TLS) によって暗号化されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) を使用して転送中に暗号化を適用していることを確認します。プレーンテキスト通信がクラスター内ブローカーノード接続に対して有効になっている場合、ルールは NON_COMPLIANT です。
4.2.1.1	PAN は、送信中に強力な暗号化で保護されます。(PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service (AWS DMS) エンドポイントが SSL 接続で設定されていることを確認します。DMS に SSL AWS 接続が設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
5.3.4	マルウェア対策のメカニズムとプロセスは、アクティブで、保守管理およびモニタリングされています。(PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup の保持期間が 365 日を超えるか、指定された保持期間に設定されていることを確認します。保持期間が MinRetentionTime (指定されている場合)、または 365 日より短い場合は NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3.3	セキュリティの脆弱性を特定し、対処します。(PCI-DSS-v4.0)	lambda-function-settings-check	ランタイム、ロール、タイムアウト、メモリサイズの AWS Lambda 関数設定が、想定値と一致していることを確認します。このルールは、「Image」パッケージタイプの関数と、「OS 専用ランタイム」に設定されたランタイムの関数を無視します。Lambda 関数の設定が期待値と一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3.3	セキュリティの脆弱性を特定し、対処します。(PCI-DSS-v4.0)	eks-cluster-oldest-supported-version	Amazon Elastic Kubernetes Service (EKS) クラスターが、サポートされているバージョンで最も古いものを実行していることを確認します。EKS クラスターがサポートされている最も古いバージョンを実行している場合 (パラメータ 「oldestVersionSupported」に等しい)、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront ディストリビューションがウェブアプリケーションファイアウォール (WAF) または WAFv2 ウェブアクセスコントロールリスト (ACL) に関連付けられていることを確認します。CloudFront ディストリビューションが WAF ウェブ ACL に関連付けられていない場合、ルールは NON_COMPLIANT です。
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	wafv2-webacl-not-empty	WAFv2 ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていない場合、ルールは NON_COMPLIANT です。
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	wafv2-rulegroup-not-empty	WAFv2 ルールグループにルールが含まれていることを確認します。WAFv2 ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
6.4.1	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF グローバルルールにいくつかの条件が含まれていることを確認します。WAF グローバルルール内に条件がない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront ディストリビューションがウェブアプリケーションファイアウォール (WAF) または WAFv2 ウェブアクセスコントロールリスト (ACL) に関連付けられていることを確認します。CloudFront ディストリビューションが WAF ウェブ ACL に関連付けられていない場合、ルールは NON_COMPLIANT です。
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	wafv2-webacl-not-empty	WAFv2 ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていない場合、ルールは NON_COMPLIANT です。
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	wafv2-rulegroup-not-empty	WAFv2 ルールグループにルールが含まれていることを確認します。WAFv2 ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
6.4.2	パブリック向けウェブアプリケーションは、攻撃から保護されています。(PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF グローバルルールにいくつかの条件が含まれていることを確認します。WAF グローバルルール内に条件がない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.5.5	すべてのシステムコンポーネントへの変更は安全に管理されます。(PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-disabled	Lambda コンピューティングプラットフォームのデプロイグループがデフォルトのデプロイ設定を使用していることを確認します。デプロイグループが「CodeDeployDefault.LambdaAllAtOnce」のデプロイ設定を使用している場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.5.5	すべてのシステムコンポーネントへの変更は安全に管理されます。(PCI-DSS-v4.0)	codepipeline-deployment-count-check	AWS CodePipeline の最初のデプロイステージで、少なくとも 1 つのデプロイが実行されていることを確認します。これは、継続的なデプロイアクティビティを監視し、定期的な更新を確保し、開発またはデプロイプロセスの問題を示す可能性のある非アクティブまたは十分に活用されていないパイプラインを特定するためです。必要に応じて、以降の残りの各ステージが、指定された数 (deploymentLimit) を超えるデプロイメントにデプロイされることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.5.6	すべてのシステムコンポーネントへの変更は安全に管理されます。(PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-disabled	Lambda コンピューティングプラットフォームのデプロイグループがデフォルトのデプロイ設定を使用していることを確認します。デプロイグループが「CodeDeployDefault.LambdaAllAtOnce」のデプロイ設定を使用している場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.5.6	すべてのシステムコンポーネントへの変更は安全に管理されます。(PCI-DSS-v4.0)	codepipeline-deployment-count-check	AWS CodePipeline の最初のデプロイステージで、少なくとも 1 つのデプロイが実行されていることを確認します。これは、継続的なデプロイアクティビティを監視し、定期的な更新を確保し、開発またはデプロイプロセスの問題を示す可能性のある非アクティブまたは十分に活用されていないパイプラインを特定するためです。必要に応じて、以降の残りの各ステージが、指定された数 (deploymentLimit) を超えるデプロイメントにデプロイされることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	shield-drt-access	Shield Response Team (SRT) がアカウントにアクセスできることを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	shield-drt-access	Shield Response Team (SRT) がアカウントにアクセスできることを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.2	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.2.4	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	Secrets Manager シークレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	shield-drt-access	Shield Response Team (SRT) がアカウントにアクセスできることを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.5	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.2.5.1	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	Secrets Manager シークレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.6	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.2.6	システムコンポーネントとデータへのアクセスは適切に定義され、割り当てられます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	shield-drt-access	Shield Response Team (SRT) がアカウントにアクセスできることを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.1	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	shield-drt-access	Shield Response Team (SRT) がアカウントにアクセスできることを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.2	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	shield-drt-access	Shield Response Team (SRT) がアカウントにアクセスできることを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
7.3.3	システムコンポーネントとデータへのアクセスは、アクセスコントロールシステム (複数可) を介して管理されます。(PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。
8.2.1	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.1	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	環境変数 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY がプロジェクトに含まていないことを確認します。プロジェクト環境変数にプレーンテキストの認証情報が含まれている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.2	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	AWS Secrets Manager シークレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.2.4	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.4	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.2.5	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.5	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.2.6	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	AWS Secrets Manager シークレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	shield-drt-access	Shield Response Team (SRT) がアカウントにアクセスできることを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.7	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	shield-drt-access	Shield Response Team (SRT) がアカウントにアクセスできることを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-imdsv2-check	Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのメタデータのバージョンが、Instance Metadata Service Version 2 (IMDSv2) で設定されていることを確認します。HttpTokens が「optional」に設定されている場合、ルールは NON_COMPLIANT です。
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Management (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	autoscaling-launchconfig-requires-imdsv2	IMDSv2 のみが有効になっていることを確認します。メタデータのバージョンが起動設定に含まれていない場合、またはメタデータ V1 と V2 の両方が有効になっている場合、このルールは非準拠です。
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.2.8	ユーザーおよび管理者のユーザー識別と関連するアカウントは、アカウントのライフサイクル全体で厳密に管理されます。(PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。
8.3.10.1	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.10.1	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。
8.3.10.1	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.11	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。
8.3.11	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (EC2) インスタンスがアマゾンキーペアを使用して起動されていないことを確認します。実行中の EC2 インスタンスが key pair で起動されている場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	athena-workgroup-encrypted-at-rest	Amazon Athena ワークグループが保管中に暗号化されていることを確認します。Athena ワークグループで保管中のデータの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Amazon Neptune DB クラスターのスナップショットが暗号化されていることを確認します。Neptune クラスターのスナップショットが暗号化されていない場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Amazon Redshift クラスターが、暗号化に指定された AWS Key Management Service (AWS KMS) キーを使用していることを確認します。暗号化が有効になっていて、クラスターが kmsKeyArn パラメータで指定されたキーで暗号化されている場合、ルールは COMPLIANT です。クラスターが暗号化されていない場合、または別のキーで暗号化されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	codebuild-project-artifact-encryption	an AWS CodeBuild プロジェクトで、すべてのアーティファクトに対して暗号化が有効になっていることを確認します。プライマリまたはセカンダリ (存在する場合) のアーティファクト設定のいずれかに「encryptionDisabled」が「true」に設定されていると、ルールは NON_COMPLIANT になります。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	codebuild-project-s3-logs-encrypted	Amazon S3 Logs で設定された an AWS CodeBuild プロジェクトで、ログに対して暗号化が有効になっていることを確認します。CodeBuild プロジェクトの S3LogsConfig で「encryptionDisabled」が「true」に設定されている場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	dax-encryption-enabled	Amazon DynamoDB Accelerator (DAX) クラスターが暗号化されていることを確認します。DAX クラスターが暗号化されていない場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis データストアの AWS Database Migration Service (AWS DMS) エンドポイントで、他のエンドポイントと通信されるデータの TLS/SSL 暗号化が有効になっていることを確認します。TLS/SSL が有効でない場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	eks-secrets-encrypted	Amazon Elastic Kubernetes Service クラスターが、 AWS Key Management Service (KMS) キーを使用して Kubernetes シークレットを暗号化するように設定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	api-gw-cache-enabled-and-encrypted	Amazon API Gateway ステージのすべてのメソッドでキャッシュが有効になっているか、および暗号化されていることを確認します。Amazon API Gateway ステージのいずれかのメソッドでキャッシュが設定されていない場合、またはキャッシュが暗号化されていない場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	docdb-cluster-encrypted	Amazon DocumentDB (MongoDB 互換) クラスターでストレージ暗号化が有効になっていることを確認します。ストレージの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルが AWS Key Management Service (KMS) で暗号化されていることを確認します。Amazon DynamoDB テーブルが KMS で暗号化されていない場合、ルールは NON_COMPLIANT AWS です。暗号化された KMS キーが kmsKeyArns AWS 入力パラメータに存在しない場合も、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	dynamodb-table-encryption-enabled	Amazon DynamoDB テーブルが暗号化されていること、およびそのステータスを確認します。ステータスが有効または有効化中の場合、ルールは COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront ディストリビューションが CloudFront エッジロケーションとカスタムオリジン間の HTTPS 通信に非推奨の SSL プロトコルを使用していないことを確認します。「OriginSslProtocols」に「SSLv3」が含まれる場合、このルールは CloudFront ディストリビューションで NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront ディストリビューションがカスタムオリジンへのトラフィックを暗号化していることを確認します。「OriginProtocolPolicy」が「http-only」、または「OriginProtocolPolicy」が「match-viewer」、かつ「ViewerProtocolPolicy」が「allow-all」である場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront ディストリビューションが HTTPS を (直接またはリダイレクト経由で) 使用していることを確認します。ViewerProtocolPolicy の値が DefaultCacheBehavior または CacheBehaviors に対して「allow-all」に設定されている場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	環境変数 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY がプロジェクトに含まていないことを確認します。プロジェクト環境変数にプレーンテキストの認証情報が含まれている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Amazon DynamoDB Accelerator (DAX) クラスターの ClusterEndpointEncryptionType が TLS に設定されていることを確認します。DAX クラスターが Transport Layer Security (TLS) によって暗号化されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Amazon EKS クラスターが AWS KMS を使用して Kubernetes シークレットを暗号化するように設定されていないことを確認します。EKS クラスターに encryptionConfig リソースがない場合、または encryptionConfig がシークレットにリソースとして命名していない場合、このルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	kinesis-stream-encrypted	Amazon Kinesis Streams がサーバー側の暗号化を使用して保存時に暗号化されていることを確認します。「StreamEncryption」が存在しない場合、ルールは Kinesis ストリームに対して NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) を使用して転送中に暗号化を適用していることを確認します。プレーンテキスト通信がクラスター内ブローカーノード接続に対して有効になっている場合、ルールは NON_COMPLIANT です。
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	neptune-cluster-encrypted	Amazon Neptune DB クラスターでストレージ暗号化が有効になっていることを確認します。ストレージの暗号化が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.2	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service (AWS DMS) エンドポイントが SSL 接続で設定されていることを確認します。DMS に SSL AWS 接続が設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service (Amazon S3) バケットポリシーで、他の AWS アカウントのプリンシパルに対して、バケット内のリソースに対するブロックリストに登録されたバケットレベルおよびオブジェクトレベルのアクションが許可されていないことを確認します。例えば、このルールは、Amazon S3 バケットポリシーが、バケット内のオブジェクトに対して s3:GetBucket* アクションと s3:DeleteObject の実行を別の AWS アカウントに許可していないことを確認します。ブロックリストに登録されているアクションが Amazon S3 バケットポリシーによって許可されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service (S3) バケットポリシーが、指定するコントロール Amazon S3 バケットポリシー以外でアカウント間の他のアクセスを許可していないことを確認します。
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	shield-drt-access	Shield Response Team (SRT) がアカウントにアクセスできることを確認します AWS 。 AWS Shield Advanced が有効になっていても SRT アクセスのロールが設定されていない場合、ルールは NON_COMPLIANT です。
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	iam-policy-in-use	IAM ポリシー ARN が、IAM ユーザー、1 人以上の IAM ユーザーを持つ IAM グループ、または 1 つ以上の信頼されたエンティティを持つ IAM ロールにアタッチされていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune クラスターで AWS Identity and Access Management (IAM) データベース認証が有効になっていることを確認します。Amazon Neptune クラスターで IAM データベース認証が有効になっていない場合、ルールは NON_COMPLIANT です。
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) クラスターで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS クラスターで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 インスタンスに AWS Identity and Access Managemen t (IAM) プロファイルがアタッチされていることを確認します。IAM プロファイルが EC2 インスタンスにアタッチされていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.4	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで AWS Identity and Access Management (IAM) 認証が有効になっていることを確認します。Amazon RDS インスタンスで IAM 認証が有効になっていない場合、ルールは NON_COMPLIANT です。
8.3.5	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.5	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。
8.3.5	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.7	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.3.7	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.7	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.3.9	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.3.9	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。
8.3.9	ユーザーと管理者の強力な認証が確立されたうえで、管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.4.1	CDE へのアクセスを保護するために、多要素認証 (MFA) が実装されています。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。
8.4.2	CDE へのアクセスを保護するために、多要素認証 (MFA) が実装されています。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。
8.4.3	CDE へのアクセスを保護するために、多要素認証 (MFA) が実装されています。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.6.3	アプリケーションアカウントとシステムアカウント、および関連する認証要素の使用は厳しく管理されます。(PCI-DSS-v4.0)	access-keys-rotated	アクティブな IAM アクセスキーが、maxAccessKeyAge で指定された日数内にローテーション (変更) されることを確認します。アクセスキーが指定した期間内にローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
8.6.3	アプリケーションアカウントとシステムアカウント、および関連する認証要素の使用は厳しく管理されます。(PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	Secrets Manager のシー AWS クレットがローテーションスケジュールに従って正常にローテーションされたことを確認します。Secrets Manager はローテーションが行われる日付を計算します。日付が過ぎてシークレットがローテーションされるまで、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.6.3	アプリケーションアカウントとシステムアカウント、および関連する認証要素の使用は厳しく管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager のシークレットが、指定した日数内にローテーションされていることを確認します。シークレットが maxDaysSinceRotation の日数を超えてローテーションされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 手動 DB クラスタースナップショットがパブリックでないことを確認します。既存および新規の Neptune スナップショットがパブリックの場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。
A1.1.2	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API が、ルールパラメータ「endpointConfigurationType」で指定されたタイプであることを確認します。REST API がルールパラメータで設定されたエンドポイントタイプと一致しない場合、ルールは NON_COMPLIANT を返します。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront ディストリビューションがウェブアプリケーションファイアウォール (WAF) または WAFv2 ウェブアクセスコントロールリスト (ACL) に関連付けられていることを確認します。CloudFront ディストリビューションが WAF ウェブ ACL に関連付けられていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront ディストリビューションに関連付けられている証明書が、デフォルトの SSL 証明書であることを確認します。CloudFront ディストリビューションでデフォルトの SSL 証明書が使用される場合、ルールは NON_COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS Network Firewall ポリシーに、フラグメント化されたパケットに対するユーザー定義のステートレスデフォルトアクションが設定されていることを確認します。フラグメント化されたパケットのステートレスデフォルトアクションがユーザー定義のデフォルトアクションと一致しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service (Amazon RDS) DB セキュリティグループがデフォルトであることを確認します。デフォルトの DB セキュリティグループではない DB セキュリティグループが存在する場合、ルールは NON_COMPLIANT になります。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud (Amazon EC2) トランジットゲートウェイで「AutoAcceptSharedAttachments」が有効になっていることを確認します。「AutoAcceptSharedAttachments」が「有効」に設定されている場合、ルールは、トランジットゲートウェイに対して NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service (Amazon EKS) エンドポイントがパブリックアクセス可能になっていないことを確認します。エンドポイントがパブリックである場合、ルールは NON_COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	restricted-ssh	注意: このルールでは、ルール識別子 (INCOMING_SSH_DISABLED) とルール名 (restricted-ssh) が異なります。セキュリティグループの受信 SSH トラフィックがアクセス可能であることを確認します。セキュリティグループの受信 SSH トラフィックの IP アドレスが制限されている場合 (0.0.0.0/0 または ::/0 以外の CIDR)、ルールは COMPLIANT です。それ以外の場合は、NON_COMPLIANTです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs が AWS WAFv2 ウェブアクセスコントロールリスト (ACLs) に関連付けられていることを確認します。ウェブ ACL に関連付けられていない場合、 AWS AppSync API のルールは NON_COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket のソースリポジトリの URL に、サインイン用の認証情報が含まれていないことを確認します。URL にサインイン情報が含まれている場合、ルールは NON_COMPLIANT です。それ以外の場合、COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer が AWS Certificate Manager が提供する SSL 証明書を使用していることを確認します。このルールを使用するには、Classic Load Balancer と共に SSL または HTTPS リスナーを使用する必要があります。注意 - このルールは、Classic Load Balancer にのみ適用されます。このルールは Application Load Balancer および Network Load Balancer を確認しません。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	ネットワークアクセスコントロールリスト (NACL) の SSH/RDP イングレストラフィックに対するデフォルトポートが制限付きであることを確認します。NACL インバウンドエントリがポート 22 または 3389 についてソース TCP または UDP CIDR ブロックを許可する場合、ルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれていることを確認します。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、ルールは NON_COMPLIANT になります。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic ルールグループにいくつかのルールが含まれていることを確認します。ルールグループにルールがない場合、ルールは NON_COMPLIANT になります。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF グローバルルールにいくつかの条件が含まれていることを確認します。WAF グローバルルール内に条件がない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS クライアント VPN 承認ルールがすべてのクライアントへの接続アクセスを許可していないことを確認します。「AccessAll」が存在し、true に設定されている場合、ルールは NON_COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが、承認された仮想プライベートクラウド (Amazon VPC) にアタッチされていることを確認します。インターネットゲートウェイが承認された VPC にアタッチされている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
A1.1.3	マルチテナントサービスプロバイダーは、すべての顧客環境とデータを保護および分離します。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 ステージで、アクセスログが有効であることを確認します。ステージ設定に「accessLogSettings」が存在しない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon CloudFront ディストリビューションが、Amazon S3 バケットにアクセスログを提供するように設定されていることを確認します。CloudFront ディストリビューションにログ記録が設定されていない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。次のすべてを満たす証跡が少なくとも 1 つある場合、このルールは COMPLIANT です:

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていることを確認します。Neptune クラスターで、監査ログ用に CloudWatch ログのエクスポートが有効になっていない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	ecs-task-definition-log-configuration	アクティブな ECS タスクの定義に、logConfiguration が設定されていることを確認します。アクティブな ECSTaskDefinition に logConfiguration リソースが定義されていない場合、または少なくとも 1 つのコンテナ定義で logConfiguration の値が NULL の場合、このルールは NON_COMPLIANT になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	cloudtrail-enabled	注意: このルールでは、ルール識別子 (CLOUD_TRAIL_ENABLED) とルール名 (cloudtrail-enabled) が異なります。 AWS アカウントで AWS CloudTrail 証跡が有効になっていることを確認します。証跡が有効でない場合、ルールは NON_COMPLIANT です。オプションで、ルールは特定の S3 バケット、Amazon Simple Notification Service (Amazon SNS) トピック、CloudWatch ロググループを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	注意: このルールでは、ルール識別子 (MULTI_REGION_CLOUD_TRAIL_ENABLED) とルール名 (multi-region-cloudtrail-enabled) が異なります。マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。追跡が入力パラメータと一致しない場合、ルールは NON_COMPLIANT です。ExcludeManagementEventSources フィールドが空でない場合、または KMS イベントや Amazon RDS Data API イベントなどの管理イベントを除外するように AWS CloudTrail AWS が設定されている場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API でログ記録が有効になっていることを確認します。ログ記録が有効されていない場合、または 'FieldLogLevel' が ERROR でも ALL でもない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF クラシックグローバルウェブアクセスコントロールリスト (ウェブ ACLs) でログ記録が有効になっていることを確認します。ログ記録が有効になっていない場合、ルールはグローバルウェブ ACL に対して NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ ブローカーで Amazon CloudWatch 監査ログが有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ ブローカーで CloudWatch 監査ログ記録が有効になっていることを確認します。ブローカーで監査ログが有効になっていない場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、ログが有効な状態で設定されていることを確認します。Amazon EKS クラスターのログが、すべてのログタイプに対して有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	AWS Elastic Beanstalk 環境が Amazon CloudWatch Logs にログを送信するように設定されていることを確認します。「StreamLogs」の値が「false」の場合、ルールは NON_COMPLIANT です。
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions マシンでログ記録が有効になっていることを確認します。ステートマシンのログ記録が有効にされていない場合、またはログ記録設定が指定された最小レベルを満たしていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A1.2.1	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall ファイアウォールでログ記録が有効になっていることを確認します。ログタイプが設定されていない場合、ルールは NON_COMPLIANT です。ルールがチェックするログタイプを指定できます。
A1.2.3	マルチテナントサービスプロバイダーは、すべての顧客のログ記録とインシデント対応を容易にします。(PCI-DSS-v4.0)	security-account-information-provided	AWS アカウントの連絡先にセキュリティ連絡先情報を提供していることを確認します。アカウント内のセキュリティの連絡先情報が指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.2.5.1	PCI DSS スコープは文書化され、検証されます。(PCI-DSS-v4.0)	macie-auto-sensitive-data-discovery-check	Amazon Macie で機密データの自動検出が有効になっていることを確認します。機密データの自動検出が無効になっている場合、ルールは NON_COMPLIANT です。このルールは管理者アカウントに適用され、メンバーアカウントには NOT_APPLICABLE です。
A3.2.5.1	PCI DSS スコープは文書化され、検証されます。(PCI-DSS-v4.0)	macie-status-check	Amazon Macie がリージョンごとにアカウントで有効になっていることを確認します。「status」属性が「ENABLED」に設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.2.5.2	PCI DSS スコープは文書化され、検証されます。(PCI-DSS-v4.0)	macie-auto-sensitive-data-discovery-check	Amazon Macie で機密データの自動検出が有効になっていることを確認します。機密データの自動検出が無効になっている場合、ルールは NON_COMPLIANT です。このルールは管理者アカウントに適用され、メンバーアカウントには NOT_APPLICABLE です。
A3.2.5.2	PCI DSS スコープは文書化され、検証されます。(PCI-DSS-v4.0)	macie-status-check	Amazon Macie がリージョンごとにアカウントで有効になっていることを確認します。「status」属性が「ENABLED」に設定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation スタックが Amazon SNS トピックにイベント通知を送信していることを確認します。オプションで、指定された Amazon SNS トピックが使用されていることを確認します。CloudFormation スタックが通知を送信しない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。
A3.3.1	PCI DSS は、通常業務 (BAU) アクティビティに組み込まれています。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 手動 DB クラスタースナップショットがパブリックでないことを確認します。既存および新規の Neptune スナップショットがパブリックの場合、ルールは NON_COMPLIANT です。
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 手動クラスタースナップショットがパブリックでないことを確認します。Amazon DocumentDB 手動クラスタースナップショットがパブリックである場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	バックアップ/リカバリ・ポイントの手動削除/無効化	バックアップボールトに、リカバリポイントの削除を防ぐリソースベースのポリシーが添付されていることを確認します。バックアップボールトにリソースベースのポリシーがない場合、または適切な「拒否」ステートメント (backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAccessPolicy アクセス許可を持つステートメント) がないポリシーがある場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR のアカウントでパブリックアクセスのブロック設定が有効になっていることを確認します。BlockPublicSecurityGroupRules が False の場合、このルールは NON_COMPLIANT に、True の場合、ポート 22 以外のポートは PermittedPublicSecurityGroupRuleRanges に一覧表示されます。
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	secretsmanager-secret-unused	AWS Secrets Manager シークレットが、指定された日数内にアクセスされていることを確認します。シークレットが「unusedForDays」の日数以内にアクセスされていない場合、ルールは NON_COMPLIANT です。デフォルト値は 90 日です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 Access Points で、パブリックアクセスブロック設定が有効になっていることを確認します。S3 アクセスポイントに対してパブリックアクセスブロック設定が有効になっていない場合、ルールは NON_COMPLIANT です。
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	s3-account-level-public-access-blocks	必要なパブリックアクセスブロック設定がアカウントレベルから設定されていることを確認します。以下に設定されているフィールドが、設定項目の対応するフィールドと一致しない場合、ルールは NON_COMPLIANT のみです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.4.1	カード所有者データ環境への論理アクセスは、制御および管理されます。(PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service (Amazon S3) バケットバージョニング設定で MFA 削除が有効になっていることを確認します。MFA 削除が有効でない場合、ルールは NON_COMPLIANT です。
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST API で AWS X-Ray トレースが有効になっていることを確認します。APIs X-Ray トレースが有効になっている場合、このルールは COMPLIANT です。そうでない場合は、NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation スタックが Amazon SNS トピックにイベント通知を送信していることを確認します。オプションで、指定された Amazon SNS トピックが使用されていることを確認します。CloudFormation スタックが通知を送信しない場合、ルールは NON_COMPLIANT です。
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	詳細モニタリングが EC2 インスタンスに対して有効になっていることを確認します。詳細モニタリングが有効になっていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch のアラームに ALARM、INSUFFICIENT_DATA、または OK の状態に設定されたアクションがあることを確認します。オプションで、指定した ARN に一致するアクションがあることを確認します。アラームまたはオプションパラメータにアクションが指定されていない場合、ルールは NON_COMPLIANT です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	リソースタイプに、名前付きメトリクスの CloudWatch アラームがあることを確認します。リソースタイプとして、EBS ボリューム、EC2 インスタンス、Amazon RDS クラスター、または S3 バケットを指定できます。名前付きメトリクスにリソース ID と CloudWatch アラームがある場合、ルールは COMPLIANT になります。
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	特定のメトリクス名を持つ CloudWatch アラームに指定された設定があることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 ルールグループの Amazon CloudWatch セキュリティメトリクス収集が有効になっていることを確認します。[visibilityConfig.CloudWatchMetricsEnenabled] フィールドが false に設定されている場合、ルールは NON_COMPLIANT です。
A3.5.1	疑わしいイベントが特定され、対応されます。(PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	エンドポイントのトピックに送信される通知メッセージの配信ステータスについて、Amazon Simple Notification Service (SNS) ログが有効になっていることを確認します。メッセージの配信ステータス通知が有効でない場合、ルールは NON_COMPLIANT です。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for PCI DSS 4.0 (グローバルリソースタイプを含む)」で入手できます。

パブリックにアクセス可能なリソースの運用のベストプラクティス

このコンフォーマンスパックは、パブリックにアクセス可能なリソースを特定するのに役立ちます。

でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Publicly Accessible Resources」で入手できます。

RBI の「Cyber Security Framework for UCBs」に関する運用上のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、インド準備銀行 (RBI) の「Cyber Security Framework for Urban Cooperative Banks (UCBs)」と、 AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の RBI Cyber Security Framework for UCBs コントロールに関連付けられます。RBI の「Cyber Security Framework for UCB」によるコントロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.1)	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーション

コントロール ID	AWS 設定ルール	ガイダンス
		のインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
Annex_I (1.1)	account-part-of-organizations	AWS Organizations AWS アカウント 内の の一元管理は、アカウントが準拠していることを確保するのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。
Annex_I (1.1)	ecr-private-tag-immutability-enabled	Elastic Container Repository (ECR) のタグ不変性を有効にして、ECR イメージのイメージタグが上書きされないようにします。以前は、タグが上書きされる可能性があり、手作業でイメージを一意に識別するための手法が必要でした。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
Annex_I (1.3)	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	api-gw-cache-enabled-and-encrypted	保管中のデータを保護するため、API Gateway ステージのキャッシュで暗号化が有効になっていることを確認します。機密データは API のメソッドでキャプチャされる可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認してください。
Annex_I (1.3)	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
Annex_I (1.3)	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
Annex_I (1.3)	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。
Annex_I (1.3)	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。
Annex_I (1.3)	バックアップ/リカバリ・ポイント暗号化	AWS Backup 復旧ポイントで暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	codebuild-project-artifact-encryption	保管中の機密データを保護するために、 AWS CodeBuild アーティファクトに対して暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	codebuild-project-s3-logs-encrypted	保管中の機密データを保護するために、Amazon S3 に保存されている AWS CodeBuild ログに対して暗号化が有効になっていることを確認します。
Annex_I (1.3)	opensearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service ドメインで暗号化が有効になっていることを確認します。
Annex_I (1.3)	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。
Annex_I (1.3)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	dynamodb-table-encrypted-kms	Amazon DynamoDB テーブルで、暗号化が有効になっていることを確認します。これらのテーブルには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。デフォルトでは、DynamoDB テーブルは AWS 所有のカスタマーマスターキー (CMK) で暗号化されます。
Annex_I (1.3)	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	elasticsearch-encrypted-at-rest	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon OpenSearch Service (OpenSearch Service) ドメインで暗号化が有効になっていることを確認します。
Annex_I (1.3)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service のノード間の暗号化を有効にします。ノード間の暗号化により、Amazon Virtual Private Cloud (Amazon VPC) 内のすべての通信で TLS 1.2 暗号化が有効になります。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
Annex_I (1.3)	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKsが AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	rds-snapshot-encrypted	Amazon Relational Database Service (Amazon RDS) スナップショットで、暗号化が有効になっていることを確認します。機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	rds-storage-encrypted	保管中のデータを保護するため、Amazon Relational Database Service (Amazon RDS) インスタンスで暗号化が有効になっていることを確認します。Amazon RDS インスタンスには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
Annex_I (1.3)	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
Annex_I (1.3)	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	sagemaker-endpoint-configuration-kms-key-configured	保管中のデータを保護するため、SageMaker エンドポイントで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker エンドポイントには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	sagemaker-notebook-instance-kms-key-configured	保管中のデータを保護するため、SageMaker ノートブックで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。SageMaker ノートブックには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要であることを確認してください。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
Annex_I (1.3)	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Annex_I (1.3)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。
Annex_I (1.3)	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。
Annex_I (1.3)	no-unrestricted-route-to-igw	Amazon EC2 ルートテーブルで、インターネットゲートウェイへの無制限のルートがないことを確認します。Amazon VPC 内のワークロードのインターネットへのアクセスを削除または制限すると、環境内の意図しないアクセスを減らすことができます。
Annex_I (1.3)	redshift-cluster-kms-enabled	保管中のデータを保護するため、Amazon Redshift クラスターで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。Redshift クラスターには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
Annex_I (1.3)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
Annex_I (1.3)	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他の サービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
Annex_I (1.3)	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
Annex_I (1.3)	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。
Annex_I (1.3)	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。
Annex_I (1.3)	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (1.3)	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
Annex_I (1.3)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (5.1)	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。
Annex_I (5.1)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
Annex_I (5.1)	waf-regional-rule-not-empty	AWS WAF に空ではないルールがあることを確認します。条件のないルールは、意図しない動作を引き起こす可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (5.1)	waf-regional-rulegroup-not-empty	AWS WAF に空ではないルールグループがあることを確認します。空のルールグループは、意図しない動作を引き起こす可能性があります。
Annex_I (5.1)	waf-regional-webacl-not-empty	AWS WAF にアタッチされたウェブ ACL には、ウェブリクエストを検査および制御するためのルールとルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、WAF による検出または処理なしに通過します。
Annex_I (5.1)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (5.1)	api-gw-associated-with-waf	AWS WAF では、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルール (ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる) を設定できます。Amazon API Gateway のステージが WAF のウェブ ACL に関連付けられ、悪意のある攻撃から保護されていることを確認します。
Annex_I (5.1)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (5.1)	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。
Annex_I (6)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (6)	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
Annex_I (6)	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (6)	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。
Annex_I (6)	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (6)	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automated SnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。
Annex_I (6)	vuln-management-plan-exists (process check)	環境の脆弱性に対処するためのプロセスを正式に定義するため、脆弱性管理計画が策定され、実施されていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.1)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
Annex_I (7.1)	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.1)	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
Annex_I (7.1)	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.1)	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.2)	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.3)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
Annex_I (7.4)	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。
Annex_I (7.4)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.4)	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
Annex_I (7.4)	cloudtrail-s3-dataevents-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。
Annex_I (7.4)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.4)	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。
Annex_I (7.4)	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.4)	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。
Annex_I (7.4)	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.4)	opensearch-audit-logging-enabled	Amazon OpenSearch Service ドメインで監査ログ作成が有効になっていることを確認します。監査ロギング作成により、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch ドメインでのユーザーアクティビティを追跡できます。
Annex_I (7.4)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
Annex_I (7.4)	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.4)	multi-region-cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。
Annex_I (7.4)	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.4)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。
Annex_I (7.4)	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.4)	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (7.4)	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。
Annex_I(10.2)	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (12)	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。
Annex_I (12)	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (12)	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。
Annex_I (12)	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (12)	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
Annex_I (12)	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (12)	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要件を反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (12)	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。
Annex_I (12)	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (12)	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
Annex_I (12)	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	AWS 設定ルール	ガイダンス
Annex_I (12)	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for RBI Cyber Security Framework for UCBs」で入手できます。

RBI の「MD-ITF」の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、インド準備銀行 (RBI) の「Master Direction – Information Technology Framework」と AWS マネージド Config ルール間のマッピングの例を示します。各 Config ルールは特定の AWS リソースに適用され、1 つ以上の RBI Master Direction – Information Technology Framework コントロールに関連付けられます。RBI の「Master Direction - Information Technology Framework」によるコント

ロールを、複数の Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (a)	情報資産の識別と分類。	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
3.1 (a)	情報資産の識別と分類。	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。
3.1 (a)	情報資産の識別と分類。	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (a)	情報資産の識別と分類。	ecr-private-tag-immutability-enabled	Elastic Container Repository (ECR) のタグ不変性を有効にして、ECR イメージのイメージタグが上書きされないようにします。以前は、タグが上書きされる可能性があり、手作業でイメージを一意に識別するための手法が必要でした。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。
3.1 (c)	ロールベースのアクセスコントロール	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムやアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーではなく、 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基本的なセキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
3.1 (c)	ロールベースのアクセスコントロール	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、ポリシーに「リソース」：「*」ではなく「アクション」：「*」の「効果」：「許可」を含めることを制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
3.1 (c)	ロールベースのアクセスコントロール	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーは、システムおよびアセットへのアクセスを制御するために、グループまたはロールにのみアタッチされます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
3.1 (c)	ロールベースのアクセスコントロール	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (c)	ロールベースのアクセスコントロール	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager シークレットのローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
3.1 (c)	ロールベースのアクセスコントロール	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (g)	インシデント管理	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (g)	インシデント管理	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (g)	インシデント管理	alb-waf-enabled	ウェブアプリケーションを保護するために、Elastic Load Balancer (ELB) で AWS WAF が有効になっていることを確認します。WAF は、一般的なウェブの脆弱性からウェブアプリケーションや API を保護するのに役立ちます。これらのウェブの脆弱性は、お客様の環境で可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (g)	インシデント管理	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (g)	インシデント管理	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
3.1 (h)	追跡	api-gw-execution-logging-enabled	API Gateway のログ記録では、API にアクセスしたユーザーと API にアクセスした方法に関する詳細ビューが表示されます。このインサイトにより、ユーザーアクティビティを可視化することができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
3.1 (h)	追跡	codebuild-project-logging-enabled	ビルド出力ログが Amazon CloudWatch または Amazon Simple Storage Service (Amazon S3) のいずれかに送信されるように、Security AWS CodeBuild プロジェクトのログ記録が有効になっています。ビルド出力ログによって、ビルドプロジェクトに関する詳細情報が得られます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。OpenSearch Service のエラーログは、セキュリティとアクセス監査や可用性の問題の診断に役立ちます。
3.1 (h)	追跡	redshift-audit-logging-enabled	Amazon Redshift クラスターの接続とユーザーアクティビティに関する情報をキャプチャするには、監査ログ作成が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。AWS サービスを呼び出し AWS アカウントたユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、AWS CloudTrail レコードコンテンツ内に表示されます。
3.1 (h)	追跡	cloudtrail-s3-data events-enabled	Simple Storage Service (Amazon S3) のデータイベントを収集することで、異常性の高いアクティビティを検出できます。詳細には、Amazon S3 バケットにアクセスした AWS アカウント 情報、IP アドレス、イベント発生時刻が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	cw-loggroup-retention-period-check	トラブルシューティングとフォレンジック調査を実行するため、ロググループでイベントログデータの最小期間が保持されていることを確認します。利用可能な過去のイベントログデータを入手できない場合、悪意のあるイベントの再構築と特定が困難になります。
3.1 (h)	追跡	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service のドメインでエラーログが有効になっており、保持と応答のために Amazon CloudWatch Logs にストリーミングされていることを確認します。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	elb-logging-enabled	Elastic Load Balancing でのアクティビティは、環境内の通信の中心となるポイントです。ELB ログ記録が有効になっていることを確認します。収集されたデータから、ELB に送信されるリクエストについての詳細情報が得られます。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	multi-region-cloudtrail-enabled	AWS CloudTrail は、AWS マネジメントコンソールのアクションと API コールを記録します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。MULTI_REGION_CLOUD_TRAIL_ENABLED が有効になっている場合、CloudTrail はすべての AWS リージョンから S3 バケットにログファイルを配信します。さらに、 が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンに同じ証跡を作成します。その結果、アクションを実行しなくても、新しいリージョンの API アクティビティを含むログファイルを受け取ることができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	rds-logging-enabled	環境内でログ記録とモニタリングを行うため、Amazon Relational Database Service (Amazon RDS) でログ記録を有効にします。Amazon RDS のログ記録を使用すると、接続、切断、クエリ、クエリされたテーブルなどのイベントをキャプチャできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	wafv2-logging-enabled	環境内のログ記録とモニタリングに役立つように、リージョンおよびグローバルウェブ ACLs で AWS WAF (V2) ログ記録を有効にします。AWS WAF ログ記録は、ウェブ ACL によって分析されるトラフィックに関する詳細情報を提供します。ログには、 AWS WAF が AWS リソースからリクエストを受信した時間、リクエストに関する情報、および各リクエストが一致したルールのアクションが記録されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (h)	追跡	redshift-cluster-configuration-check	保管中のデータを保護するため、Amazon Redshift クラスターで暗号化が有効になっていることを確認します。また、必要な設定が Amazon Redshift クラスターにデプロイされていることを確認する必要があります。監査ログを有効にして、データベース内の接続とユーザーアクティビティに関する情報を提供します。このルールでは、clusterDbEncrypted (Config デフォルト: TRUE) と loggingEnabled (Config デフォルト:TRUE) の値が設定されている必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (i)	パブリックキー構造	acm-certificate-expiration-check	X509 証明書が AWS ACM によって発行されるようにすることで、ネットワークの整合性が保護されていることを確認します。これらの証明書は有効で、期限切れではない必要があります。このルールには daysToExpiration の値が必要です (AWS 基礎セキュリティのベストプラクティス値: 90)。実際の値には、組織のポリシーを反映する必要があります。
3.1 (i)	パブリックキー構造	alb-http-drop-invalid-header-enabled	Elastic Load Balancing (ELB) が、http ヘッダーを削除するように設定されていることを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (i)	パブリックキー構造	alb-http-to-https-redirection-check	転送中のデータを保護するため、暗号化されていない HTTP リクエストを Application Load Balancer が HTTPS に自動的にリダイレクトするようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1 (i)	パブリックキー構造	api-gw-ssl-enabled	Amazon API Gateway REST API ステージで SSL 証明書を設定して、バックエンドシステムが API Gateway からのリクエストを認証できるようにします。
3.1 (i)	パブリックキー構造	opensearch-https-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Amazon OpenSearch Service ドメインへの接続で HTTPS が有効になっていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (i)	パブリックキー構造	elbv2-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。
3.1 (i)	パブリックキー構造	elb-acm-certificate-required	機密データが含まれている可能性があるため、転送中のデータを保護するために Elastic Load Balancing で暗号化を有効にします。 AWS Certificate Manager を使用して、 AWS サービスおよび内部リソースでパブリックおよびプライベート SSL/TLS 証明書を管理、プロビジョニング、デプロイします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (i)	パブリックキー構造	elb-tls-https-listeners-only	Elastic Load Balancing (ELB) が、SSL または HTTPS リスナーを使用して設定されるようにします。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.1 (i)	パブリックキー構造	redshift-require-tls-ssl	Amazon Redshift クラスターで、SQL クライアントに接続するために TLS/SSL 暗号化が必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.1 (i)	パブリックキー構造	s3-bucket-ssl-requests-only	転送中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで、Secure Sockets Layer (SSL) を使用するためのリクエストが必要かどうかを確認します。機密データが含まれている可能性があるため、転送中の暗号化を有効にしてデータを保護します。
3.3	Vulnerability Management	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 環境でマネージドプラットフォームの更新を有効にすると、利用可能なプラットフォームの最新の修正、更新と、環境のための機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムのセキュリティ保護のベストプラクティスです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	Vulnerability Management	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service (RDS) インスタンスで自動マイナーバージョンアップグレードを有効にすると、セキュリティパッチやバグ修正を含むリレーショナルデータベース管理システム (RDBMS) の最新のマイナーバージョンアップデートをインストールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	Vulnerability Management	redshift-cluster-maintenancesettings-check	このルールにより、Amazon Redshift クラスターで組織に適した設定が行われるようになります。具体的には、データベースの任意のメンテナンスウインドウと自動スナップショットの保持期間を設定します。このルールでは、allowVersionUpgrade を設定する必要があります。デフォルトは true です。必要に応じて、「preferredMaintenanceWindow (デフォルトは「sat: 16:00-sat: 16:30」) と automatedSnapshotRetentionPeriod (デフォルトは 1) を設定することもできます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	Vulnerability Management	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	Vulnerability Management	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	Vulnerability Management	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.3	Vulnerability Management	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5	サイバー危機管理計画	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5	サイバー危機管理計画	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5	サイバー危機管理計画	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5	サイバー危機管理計画	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager の関連付けを使用すると、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager は、マネージドインスタンスに設定状態を割り当て、オペレーティングシステムのパッチレベル、ソフトウェアのインストール、アプリケーション設定、および環境に関するその他の詳細のベースラインを設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.5	サイバー危機管理計画	ec2-managedinstance-patch-compliance-status-check	このルールを有効にすると、Amazon Elastic Compute Cloud (Amazon EC2) の脆弱性の特定とドキュメント化ができます。このルールは、組織のポリシーと手順で義務付けられている Systems AWS Manager の Amazon EC2 インスタンスパッチコンプライアンスをチェックします。
3.9	IT Risk Assessment	annual-risk-assessment-performed (process check)	年に 1 回、組織のリスク評価を実施します。リスク評価は、組織に影響を及ぼす可能性のある特定のリスクや脆弱性の影響を判断するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
3.12	トレーニング	security-awareness-program-exists (Process Check)	組織のセキュリティ意識向上プログラムを確立して維持します。セキュリティ意識向上プログラムは、さまざまなセキュリティ侵害やインシデントから組織を保護する方法を従業員に教育するものです。
4.4 (g)	不正分析 - 疑わしい取引の分析、横領、窃盗またはマネーロンダリングの疑い、資産の不正流用、財務記録の操作など。RBI に不正を報告するという規制要件は、システム主導である必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	clb-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	elbv2-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	lambda-vpc-multi-az-check	AWS Lambda 関数がアカウントの Virtual Private Cloud (VPC) に接続するように設定されている場合は、Lambda AWS 関数を少なくとも 2 つの異なるアベイラビリティーゾーンにデプロイして、単一のゾーンでサービスが中断された場合に関数がイベントを処理できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	s3-bucket-default-lock-enabled	Amazon Simple Storage Service (Amazon S3) バケットで、 デフォルトでロックが有効になっていることを確認します。S3 バケットには機密データが含まれている可能性があるため、保管時にオブジェクトロックを適用してデータを保護します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	lambda-dlq-check	このルールを有効にすると、機能が失敗した場合に、Amazon Simple Queue Service (Amazon SQS) または Amazon Simple Notification Service (Amazon SNS) を介して、適切な担当者に通知できます。
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk の拡張ヘルスレポートにより、基盤となるインフラストラクチャのヘルスの変化により迅速に対応できます。これらの変更は、アプリケーションの可用性を低下させる可能性があります。Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) の最適化インスタンスは、Amazon EBS I/O 操作専用の追加容量を提供します。この最適化は、Amazon EBS I/O 操作とその他のインスタンスからのトラフィック間の競合を最小化することで、EBS ボリュームの効率的なパフォーマンスを実現します。
4.4 (h)	IT セキュリティシステムの容量とパフォーマンスの分析。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (i)	インシデントの報告とその影響、および今後そのようなイベントを再発させないための措置。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
4.4 (i)	インシデントの報告とその影響、および今後そのようなイベントを再発させないための措置。	guardduty-non-archived-findings	Amazon GuardDuty では、調査結果が重要度 (低、中、高) で分類されるため、インシデントによる影響を把握することができます。これらの分類を使用して、修復戦略と優先度を決定することができます。このルールでは、組織のポリシーで要求される場合に、アーカイブされていない結果に対して daysLowSev (Config デフォルト: 30)、daysMediumSev (Config デフォルト: 7)、daysHighSev (Config デフォルト: 1) を必要に応じて設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	バックアップ計画によって保護された aurora リソース	データのバックアッププロセスを支援するには、Amazon Aurora リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	cmk-backing-key-rotation-enabled	キーのローテーションを有効にして、暗号化期間の最後に到達した後にキーがローテーションされるようにします。
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	EC2-バックアップ計画によって保護されるリソース	データのバックアッププロセスを支援するために、Amazon Elastic Compute Cloud (Amazon EC2) リソースが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	fsx-リソース-バックアップ計画によって保護される	データのバックアッププロセスを支援するために、Amazon FSx ファイルシステムが AWS Backup プランの一部であることを確認します。AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
6.3	NBFC は、ビジネスの重要なシステムとデータセンターのために必要なバックアップサイトを設置する必要性について考慮するものとします。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling は、AWS Application Auto Scaling サービスを使用して、実際のトラフィックパターンに自動的に応答するプロビジョニングされたスループットキャパシティを調整します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み取りおよび書き込みの容量が拡張され、トラフィックの急激な増加をスロットリングなしで処理できるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	elb-cross-zone-load-balancing-enabled	Elastic Load Balancing (ELB) のクロスゾーン負荷分散を有効にして、十分な容量と可用性を維持します。クロスゾーン負荷分散により、有効な各アベイラビリティーゾーンで同じインスタンス数を維持する必要性が軽減されます。また、1 つ以上のインスタンスの消失を処理するアプリケーションの能力が向上します。
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	elb-deletion-protection-enabled	このルールにより、Elastic Load Balancing で削除保護が有効になっているかどうかを確認します。この機能を使用すると、ロードバランサーが誤って削除されたり悪意を持って削除されることで、アプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	clb-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	elbv2-multiple-az	Elastic Load Balancing (ELB) では、受信したトラフィックがアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。高可用性を確保するには、ELB に複数のアベイラビリティーゾーンのインスタンスが登録されていることを確認してください。
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	lambda-vpc-multi-az-check	AWS Lambda 関数がアカウントの Virtual Private Cloud (VPC) に接続するように設定されている場合は、Lambda AWS 関数を少なくとも 2 つの異なるアベイラビリティーゾーンにデプロイして、単一のゾーンでサービスが中断された場合に関数がイベントを処理できるようにします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	rds-instance-deletion-protection-enabled	Amazon Relational Database Service (Amazon RDS) インスタンスで、削除保護が有効になっていることを確認します。削除保護を使用すると、Amazon RDS インスタンが誤って削除されたり、悪意を持って削除されることでアプリケーションの可用性が失われることを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) のマルチ AZ のサポートにより、データベースインスタンスの可用性と耐久性が強化されます。マルチ AZ のデータベースインスタンスをプロビジョニングすると、Amazon RDS はプライマリデータベースのインスタンスを自動的に作成し、別のアベイラビリティーゾーンのスタンバイインスタンスにデータを同期的にレプリケートします。各アベイラビリティーゾーンは、物理的に独立した独自のインフラストラクチャで実行されますが、高度な信頼性を実現できるよう設計されています。インフラストラクチャに障害が発生した場合、Amazon RDS ではスタンバイへの自動フェイルオーバーが実行されるため

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			、フェイルオーバーが完了するとすぐにデータベース運用を再開できます。
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	vpc-vpn-2-tunnels-up	冗長な Site-to-Site VPN トンネルを実装することで、回復性の要件を満たすことができます。2 つのトンネルを使用することで、Site-to-Site VPN 接続の 1 つが使用できなくなった場合の接続を確保します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 つ目のカスタマーゲートウェイを使用して Amazon Virtual Private Cloud (Amazon VPC) および仮想プライベートゲートウェイへの 2 つ目の Site-to-Site VPN 接続を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling グループの Elastic Load Balancing (ELB) ヘルスチェックは、十分な容量と可用性の維持をサポートします。ロードバランサーは、定期的に ping の送信、接続の試行、リクエストの送信を実行し、Auto scaling グループ内の Amazon EC2 インスタンスのヘルスステータスをテストします。インスタンスによってレポートが返されない場合、新しい Amazon EC2 インスタンスにトラフィックが送信されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	dynamodb-throughput-limit-check	このルールを有効にすると、Amazon DynamoDB テーブルでのプロビジョンドスループットキャパシティがチェックされるようになります。これは、各テーブルがサポートできる読み取りおよび書き込みアクティビティの量です。DynamoDB はこの情報を使用して、スループット要件を満たすのに十分なシステムリソースを予約します。このルールでは、スループットがお客様のアカウントの最大限度に近づいたときにアラートが生成されます。このルールでは、accountRCUThresholdPercentage (Config デフォルト: 80) および accountWCUThresholdPercentage (Config デフォルト: 80) のパラメータを必要に応じて設定できます。実際の値には、組織

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のポリシーを反映する必要があります。
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	lambda-concurrency-check	このルールにより、Lambda 関数の同時実行数の上限と下限が確立されているかどうかを確認します。これは、関数が任意の時点で処理しているリクエスト数をベースライン化する際に役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	rds-enhanced-monitoring-enabled	Amazon Relational Database Service (Amazon RDS) を有効にすると、Amazon RDS の可用性をモニタリングできます。これにより、Amazon RDS データベースインスタンスのヘルスステータスの詳細が可視化されます。Amazon RDS ストレージが、複数の基盤となる物理デバイスを使用している場合、拡張モニタリングによって各デバイスのデータが収集されます。また、Amazon RDS データベースインスタンスがマルチ AZ 配置で実行されている場合、セカンダリホスト上の各デバイスのデータと、セカンダリホストのメトリクスが収集されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.1	IT システムは、NBFC の業務の規模や複雑さに応じて、段階的にスケールアップしていく必要があります。	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS Identity and Access Management (IAM) Access Analyzer、AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、 AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリンAWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	dms-replication-not-public	DMS レプリケーションインスタンスにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。DMS レプリケーションインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	ebs-snapshot-public-restorable-check	EBS スナップショットをパブリックに復元できないようにすることで、 AWS クラウドへのアクセスを管理します。EBS ボリュームスナップショットには機密情報が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、クラウドへのアクセスを管理します。Amazon EC2 インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	elasticsearch-in-vpc-only	Amazon OpenSearch Service (OpenSearch Service) ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイスや VPN 接続なしで、OpenSearch Service と他のサービス間に Amazon VPC 内で安全な通信ができるようになります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	emr-master-no-public-ip	Amazon EMR クラスターのマスターノードにパブリックにアクセスできないようにすることで、 AWS クラウドへのアクセスを管理します。Amazon EMR クラスターのマスターノードには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	rds-instance-public-access-check	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	rds-snapshots-public-prohibited	Amazon Relational Database Service (Amazon RDS) インスタンスが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon RDS データベースインスタンスには機密情報と原則が含まれている可能性があるため、それらのアカウントに対するアクセスコントロールが必要です。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	redshift-cluster-public-access-check	Amazon Redshift クラスターが公開されていないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。Amazon Redshift クラスターには機密情報が含まれている可能性があるため、これらのアカウントに対する原則とアクセスコントロールが必要です。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、 AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker ノートブックが直接インターネットアクセスを許可しないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。インターネットからの直接アクセスを防止することで、権限のないユーザーが機密データにアクセスするのを防ぐことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	emr-kerberos-enabled	Amazon EMR クラスターで Kerberos を有効にすることで、最小特権と職務の分離の原則に基づいてアクセス許可と認可を管理して組み込むことができます。Kerberos では、認証を必要とするサービスとユーザーをプリンシパルと呼びます。プリンシパルは Kerberos 領域内に存在します。この領域内では、Kerberos サーバーを KDC (キー配布センター) と呼びます。これは、プリンシパルが認証を行うための手段を提供するものです。KDC は、チケットを発行して認証を行います。KDC は、領域内にあるプリンシパルのデータベースに加え、プリンシパルのパスワードや、各プリンシパルに関するその他の管理情報を保持しています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
8.l	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	autoscaling-launch-config-public-ip-disabled	パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイスに関連付けられたリソースにインターネットからアクセスできます。EC2 リソースが、アプリケーションやサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	ecs-task-definition-nonroot-user	最小特権の原則の実装を支援するため、ルートユーザー以外のあるユーザーに Amazon Elastic Container Service (Amazon ECS) タスク定義へのアクセスが指定されていることを確認します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	efs-access-point-enforce-root-directory	Amazon Elastic File System (Amazon EFS) アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	efs-access-point-enforce-user-identity	最小特権の原則の実装を支援するため、Amazon Elastic File System (Amazon EFS) でユーザー適用が有効になっていることを確認します。有効になっていると、Amazon EFS では、NFS クライアントのユーザー ID およびグループ ID が、アクセスポイントですべてのファイルシステムオペレーションに対して設定されている ID に置き換えられ、この適用されたユーザー ID へのアクセスのみが許可されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud (VPC) サブネットにパブリック IP アドレスが自動的に割り当てられないようにすることで、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud この属性が有効になっているサブネットで起動される Amazon Elastic Compute Cloud (EC2) インスタンスでは、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられています。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Managemen t (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Managemen t (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	opensearch-in-vpc-only	Amazon OpenSearch Service ドメインが Amazon Virtual Private AWS Cloud (Amazon VPC) 内にあることを確認して、 クラウドへのアクセスを管理します。 Amazon Virtual Private Cloud Amazon VPC 内の Amazon OpenSearch Service のドメインによって、インターネットゲートウェイ、NAT デバイス、そして VPN 接続を必要とせずに、Amazon OpenSearch と Amazon VPC 内にある他のサービスの間での安全な通信が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
8.I	物理的/論理的なアクセスコントロールや、明確に定義されたパスワードポリシーなどの基本的なセキュリティの側面。	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.II	明確に定義されたユーザーロール	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.II	明確に定義されたユーザーロール	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.II	明確に定義されたユーザーロール	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値：true)、 RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値：true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値：true)、 RequireNumbers (AWS 基礎セキュリティのベストプラクティス値：true)、 MinimumPasswordLength (AWS 基礎セキュリティ

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			のベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。
8.II	明確に定義されたユーザーロール	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) は、最小特権と職務分離の原則をアクセス許可と認可に組み込み、ポリシーに「Resource」：「*」ではなく「Effect」：「Allow」を「Action」：「*」と含めないように制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.II	明確に定義されたユーザーロール	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。
8.II	明確に定義されたユーザーロール	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.II	明確に定義されたユーザーロール	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.III	エラーや誤用のリスクを軽減し、データ/情報の信頼性を確保するための Maker-checker の概念。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	db-instance-backup-enabled	Amazon RDS のバックアップ機能では、データベースとトランザクションログのバックアップが作成されます。Amazon RDS により、DB インスタンスクラスターのストレージボリュームのスナップショットが自動的に作成され、DB インスタンス全体がバックアップされます。このシステムでは、回復性の要件を満たす特定の保持期間を設定できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	dynamodb-in-backup-plan	データのバックアッププロセスを支援するために、Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	dynamodb-pitr-enabled	このルールを有効にして、情報がバックアップされているかどうかをチェックします。また、Amazon DynamoDB でポイントインタイムリカバリが有効になっているかどうかを確認することで、バックアップを維持します。リカバリによって、過去 35 日間のテーブルの継続的なバックアップが維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	elasticache-redis-cluster-automatic-backup-check	自動バックアップが有効になっている場合、Amazon ElastiCache はクラスターのバックアップを毎日作成します。バックアップは、組織の指定により数日間、保持することができます。自動バックアップは、データ損失を防ぐのに役立ちます。障害が発生した場合は、新しいクラスターを作成して、最新のバックアップからデータを復元できます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	rds-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Relational Database Service (Amazon RDS) インスタンスが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアッププソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (CRR) は、十分な容量と可用性の維持をサポートします。CRR により、Amazon S3 バケット間でオブジェクトを自動的に非同期コピーできるため、データの可用性が維持されます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	redshift-backup-enabled	データのバックアッププロセスを実行するため、Amazon Redshift クラスターで自動スナップショットが設定されていることを確認します。クラスターの自動スナップショットを有効にすると、Amazon Redshift はそのクラスターのスナップショットを定期的に作成します。デフォルトでは、Redshift は 8 時間ごと、または各ノードの 5 GB ごとのデータ変更、またはそのいずれか早い方のタイミングでスナップショットを作成します。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	バックアップ計画-分-頻度と分保持チェック	データのバックアッププロセスを支援するために、 AWS バックアッププランが最小頻度と保持期間に設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。このルールでは、requiredFrequencyValue (デフォルト Config: 1)、requiredretentionDays (デフォルト Config: 35)、および requiredFrequencyUnit (デフォルト Config: 日) パラメータを設定することができます。実際の値には、組織の要

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
			件を反映する必要があります。
8.IX	定期的なテストをともなうデータのバックアップの配置。	バックアップ/リカバリ・ポイントの手動削除/無効化	AWS Backup リカバリポイントに、リカバリポイントの削除を防止するリソースベースのポリシーがアタッチされていることを確認します。リソースベースのポリシーを使用してリカバリポイントの削除を防止すると、偶発的または意図的な削除を防ぐのに役立ちます。

コントロール ID	コントロールの概要	AWS 設定ルール	ガイダンス
8.IX	定期的なテストをともなうデータのバックアップの配置。	バックアップ/リカバリ・ポイントの最小保存期間チェック	データのバックアッププロセスを支援するために、 AWS バックアップリカバリポイントに最小保持期間が設定されていることを確認します。 AWS バックアップは、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。requiredetentionDays (デフォルト設定: 35) パラメータを設定できるルールです。実際の値には、組織の要件を反映する必要があります。

テンプレート

テンプレートは、GitHub の「Operational Best Practices for RBI MD-ITF」で入手できます。

セキュリティ、ID、コンプライアンスの運用のベストプラクティス

このコンフォーマンスパックには、セキュリティ、アイデンティティ、コンプライアンスサービスに基づく AWS Config ルールが含まれています。詳細については、「 のセキュリティ、アイデンティティ、コンプライアンス AWS」を参照してください。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Security, Identity, and Compliance Services」で入手できます。

サーバーレスの運用のベストプラクティス

このコンフォーマンスパックには、サーバーレスソリューションに基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices for Serverless」で入手できます。

ストレージサービスの運用のベストプラクティス

このコンフォーマンスパックには、ストレージサービスに基づく AWS Config ルールが含まれています。詳細については、「 のクラウドストレージ AWS」を参照してください。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Operational Best Practices For Storage Services」で入手できます。

SWIFT CSP の運用のベストプラクティス

コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成

できるように設計された汎用コンプライアンスフレームワークを提供します。サンプルテンプレートとしてのコンフォーマンスパックは、特定のガバナンスまたはコンプライアンス基準を準拠するようには設計されていません。お客様は、本サービスの利用が該当する法的要件および規制要件を満たしているかどうかについて、お客様自身で評価する責任を負います。

以下に、SWIFT のカスタマーセキュリティプログラム (CSP) と AWS マネージド Config ルール間のマッピングの例を示します。各 AWS Config ルールは特定の AWS リソースに適用され、1 つ以上の SWIFT CSP コントロールに関連付けられます。SWIFT CSP コントロールは、複数の AWS Config ルールに関連付けることができます。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

コントロール ID	AWS 設定ルール	ガイダンス
1.1	ec2-instance-managed-by-systems-manager	AWS Systems Manager で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理することで、組織内のソフトウェアプラットフォームとアプリケーションのインベントリを作成できます。 AWS Systems Manager を使用して、詳細なシステム設定、オペレーティングシステムのパッチレベル、サービス名とタイプ、ソフトウェアのインストール、アプリケーション名、パブリッシャーとバージョン、および環境に関するその他の詳細を提供します。
1.1	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud (Amazon EC2) インスタンスにパブリックにアクセスできないようにすることで、 クラウドへのアクセスを管理します。Amazon EC2

コントロール ID	AWS 設定ルール	ガイダンス
		インスタンスには機密情報が含まれている可能性があるため、これらのアカウントに対するアクセスコントロールが必要です。
1.1	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud (Amazon EC2) インスタンスが Amazon キーペアを使用して起動されているかどうかを確認します。これにより、認証情報が漏洩するリスクを軽減できます。キーペアのない Amazon EC2 インスタンスには、 AWS コンソールから Session Manager またはブラウザベースの SSH 接続を使用してアクセスできます。

コントロール ID	AWS 設定ルール	ガイダンス
1.1	ec2-instances-in-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを展開し、Amazon VPC 内でのインスタンスとサービス間の安全な通信を、インターネットゲートウェイ、NAT デバイス、VPN 接続を必要とせず可能にします。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。Amazon EC2 インスタンスを Amazon VPC に割り当て、アクセスを適切に管理します。

コントロール ID	AWS 設定ルール	ガイダンス
1.1	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。デフォルトのセキュリティグループのすべてのトラフィックを制限すると、 AWS リソースへのリモートアクセスを制限するのに役立ちます。
1.1	vpc-network-acl-unused-check	このルールにより、Amazon Virtual Private Cloud (Amazon VPC) のネットワークアクセスコントロールリストが使用されていることが確認されます。未使用のネットワークアクセスコントロールリストをモニタリングすることで、環境の正確なインベントリの使用と管理を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1.1	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。信頼できるソースへのポートに対するアクセスを制限しないと、システムの可用性、完全性、機密性に対する攻撃を招く可能性があります。インターネットからのセキュリティグループ内のリソースへのアクセスを制限することで (0.0.0.0/0)、内部システムへのリモートアクセスをコントロールできます。

コントロール ID	AWS 設定ルール	ガイダンス
1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) は、最小特権と職務の分離の原則をアクセス許可と認可に組み込み、すべての AWS Key Management Service キーにブロックされたアクションをポリシーに含めることを制限するのに役立ちます。タスク完了のために必要以上の特権を持つことは、最小特権と職務分離の原則に反する可能性があります。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。
1.2	iam-group-has-users-check	AWS Identity and Access Management (IAM) は、IAM グループに少なくとも 1 人のユーザーがいるようにすることで、最小特権と職務分離の原則をアクセス許可と認可に組み込むのに役立ちます。関連するアクセス許可や職務に基づいてユーザーをグループに配置することは、最小特権を組み込む方法の 1 つです。

コントロール ID	AWS 設定ルール	ガイダンス
1.2	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、すべての AWS Key Management Service キーでブロックされたアクションを許可するインラインポリシーがないことを確認します。 AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーでは、再利用可能性、バージョニング、ロールバック、アクセス許可の管理を委任できます。このルールにより、blockedActionsPatterns パラメータの設定が可能になります。（AWS 基本的なセキュリティのベストプラクティス値: kms:Decrypt、kms:ReEncryptFrom)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1.2	iam-no-inline-policy-check	AWS Identity and Access Management (IAM) ユーザー、IAM ロール、または IAM グループに、システムおよびアセットへのアクセスを制御するインラインポリシーがないことを確認します。AWS では、インラインポリシーの代わりに 管理ポリシーを使用することをお勧めします。管理ポリシーにより、再利用性、バージョニング、ロールバック、権限管理の委任が可能になります。
1.2	iam-user-no-policies-check	このルールにより、AWS Identity and Access Management (IAM) ポリシーがグループまたはロールにのみアタッチされ、システムおよびアセットへのアクセスが制御されます。グループレベルまたはロールレベルで特権を割り当てると、ID が過剰な特権を受け取ったり保持したりする機会を減らすことができます。

コントロール ID	AWS 設定ルール	ガイダンス
1.2	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループは、 AWS リソースへの送受信ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。リソースで 0.0.0.0/0 からポート 22 への入力 (またはリモート) トラフィックを許可しないようにすることで、リモートアクセスを制限できます。
1.2	nacl-no-unrestricted-ssh-rdp	ポート 22 (SSH) やポート 3389 (RDP) などのネットワークアクセスコントロールリスト (NACLs) のリモートサーバー管理ポートへのアクセスは、VPC 内のリソースへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1.2	s3-bucket-acl-prohibited	このルールでは、アクセスコントロールリスト (ACL) が Amazon S3 バケットのアクセスコントロールに使用されているかどうかを確認します。ACLsは、 AWS Identity and Access Management (IAM) より前の Amazon S3 バケットのレガシーアクセスコントロールメカニズムです。ベストプラクティスは、ACL の代わりに、IAM ポリシーまたは S3 バケットポリシーを使用して、S3 バケットへのアクセスをより簡単に管理することです。

コントロール ID	AWS 設定ルール	ガイダンス
1.2	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) サーバーアクセスのログ記録によって、ネットワークをモニタリングし、潜在的なサイバーセキュリティイベントに対応することができます。Amazon S3 バケットに対して行われたリクエストの詳細な記録をキャプチャすることで、イベントをモニタリングします。各アクセスのログレコードから、1 つのアクセスリクエストについての詳細情報を取得できます。詳細情報には、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、レスポンスのステータス、エラーコード (該当する場合) などの情報が含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
1.2	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check を有効にして、AWS クラウドへのアクセスを管理します。このルールは、Amazon S3 バケットによって付与されるアクセスが、指定したプリン AWS シパル、フェデレーティッドユーザー、サービスプリンシパル、IP アドレス、または Amazon Virtual Private Cloud (Amazon VPC) IDs によって制限されていることを確認します。
1.2	sns-topic-message-delivery-notification-enabled	環境での口グ記録の要件に対応するため、Amazon Simple Notification Service (Amazon SNS) トピックで配信ステータス通知が有効になっていることを確認します。メッセージの配信ステータスをログに記録することで、メッセージが Amazon SNS エンドポイントに配信されたかどうかの確認、Amazon SNS エンドポイントから Amazon SNS に送信された応答の特定、メッセージの滞留 (時間発行のタイムスタンプから Amazon SNS エンドポイントへの配信直前までの時間)など、運用上の洞察を深めることができます。

コントロール ID	AWS 設定ルール	ガイダンス
1.4	internet-gateway-authorized-vpc-only	インターネットゲートウェイが承認された Amazon Virtual Private AWS Cloud (Amazon VPC) にのみアタッチされるようにすることで、 クラウド内のリソースへのアクセスを管理します。 Amazon Virtual Private Cloud インターネットゲートウェイは、Amazon VPC との間の双方向インターネットアクセスを可能にしますが、これにより Amazon VPC リソースへの不正アクセスが発生する可能性があります。
1.4	restricted-common-ports	Amazon Elastic Compute AWS Cloud (Amazon EC2) セキュリティグループで共通ポートが制限されるようにすることで、 クラウド内のリソースへのアクセスを管理します。ポートへのアクセスを信頼できるソースに制限しなければ、システムの可用性、完全性、機密性に対する脅威を招く可能性があります。このルールでは、blockedPort1 - blockedPort5 パラメータを必要に応じて設定できます (Config デフォルト: 20、21、3389、3306、4333)。6.4.7

コントロール ID	AWS 設定ルール	ガイダンス
1.4	lambda-function-public-access-prohibited	AWS Lambda 関数にパブリックにアクセスできないようにすることで、 AWS クラウド内のリソースへのアクセスを管理します。パブリックアクセスにより、リソースの可用性の低下を招く可能性があります。
1.4	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールは、パブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護するのに役立ちます。このルールでは、ignorePublicAcls (Config デフォルト: True)、blockPublicPolicy (Config デフォルト: True)、blockPublicAcls (Config デフォルト: True)、および restrictPublicBuckets (Config デフォルト: True) の各パラメータを必要に応じて設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1.4	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service (Amazon S3) バケットにパブリックにアクセスできないようにすることで、AWS クラウド内のリソースへのアクセスを管理します。このルールでは、バケットレベルでのパブリックアクセスを防止することで、権限のないリモートユーザーから機密データを保護します。
1.4	s3-bucket-public-read-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。
1.4	s3-bucket-public-write-prohibited	Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを許可されたユーザー、プロセス、デバイスのみに許可することで、AWS クラウド内のリソースへのアクセスを管理します。アクセスの管理は、データの分類と一致している必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
1.4	ssm-document-not-public	AWS Systems Manager (SSM) ドキュメントが公開されていないことを確認します。これにより、SSM ドキュメントへの意図しないアクセスが許可される可能性があります。パブリック SSM ドキュメントにより、お客様のアカウント、リソース、内部プロセスに関する情報が公開される可能性があります。
2.3	ec2-imdsv2-check	Instance Metadata Service Version 2 (IMDSv2) メソッドが有効になっていることを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスメタデータのアクセスとコントロールを保護します。IMDSv2 メソッドでは、セッションベースのコントロールを使用します。IMDSv2 を使用すると、インスタンスメタデータへの変更を制限するためのコントロールを実装できます。

コントロール ID	AWS 設定ルール	ガイダンス
2.3	ec2-instance-multiple-eni-check	このルールは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに複数の ENI があるかどうかを確認します。複数の ENI が存在すると、デュアルホームインスタンス (複数のサブネットを持つインスタンス) を引き起こす可能性があります。これにより、ネットワークセキュリティの複雑性が増し、意図しないネットワークパスとアクセスが導入する可能性があります。
2.3	ec2-token-hop-limit-check	インスタンスメタデータサービス (IMDS) の HTTP PUT 応答が Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに限定されていることを確認します。IMDSv2 では、メタデータ応答ホップ制限が 1 (Config デフォルト) に設定されているため、シークレットトークンを含む PUT 応答は、インスタンスの外に移動することができません。この値が 1 より大きい場合、トークンは EC2 インスタンスから移動することができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.3	ec2-volume-inuse-check	このルールにより、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされた Amazon Elastic Block Store ボリュームが、インスタンスの終了時に削除対象としてマークされるようになります。Amazon EBS ボリュームが、アタッチされているインスタンスの終了時に削除されていない場合、最小限の機能の概念に反する可能性があります。
2.3	account-part-of-organizations	AWS Organizations AWS アカウント 内の の一元管理は、アカウントが確実に準拠するようにするのに役立ちます。アカウントの管理が一元化されていないと、アカウントの設定に一貫性がなくなり、リソースや機密データが流出する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.3	lambda-inside-vpc	Amazon Virtual Private Cloud (Amazon VPC) 内に AWS Lambda 関数をデプロイして、関数と Amazon VPC 内の他のサービス間の安全な通信を実現します。この設定では、インターネットゲートウェイ、NAT デバイス、VPN 接続を使用する必要はありません。すべてのトラフィックは AWS クラウド内に安全に保持されます。論理的な隔離により、VPC 内に存在するドメインには、パブリックエンドポイントを使用するドメインに比較して、より拡張されたセキュリティレイヤーがあります。アクセスを適切に管理するには、 AWS Lambda 関数を VPC に割り当てる必要があります。
2.3	kms-cmk-not-scheduled-for-deletion	保管中のデータを保護するため、必要なカスタマーマスターキー (CMKs) が AWS Key Management Service (AWS KMS) で削除されないようにします。キーの削除が必要になる場合があるため、このルールでは、キーが意図せずスケジュールされた場合に備えて、削除予定のすべてのキーをチェックすることができます。

コントロール ID	AWS 設定ルール	ガイダンス
2.3	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) バケットのバージョニングは、同じ Amazon S3 バケットでオブジェクトの複数のバリアントを保持するのに役立ちます。バージョニングを使用すると、Amazon S3 バケットに保存されたあらゆるオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションやアプリケーション障害から簡単に復旧できます。
2.3	secretsmanager-secret-unused	未使用の認証情報が AWS Secrets Manager に存在する場合は、最小特権の原則に違反する可能性があるため、認証情報を無効化または削除する必要があります。このルールでは、unusedForDays (Config デフォルト: 90) の値を設定できます。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
2.5A	ebs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic Block Store (Amazon EBS) ボリュームが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
2.5A	ec2-ebs-encryption-by-default	保管中のデータを保護するため、Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。これらのボリュームには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。
2.5A	efs-encrypted-check	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic File System (EFS) で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
2.5A	efs-in-backup-plan	データのバックアッププロセスを支援するために、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup プランの一部であることを確認します。 AWS Backup は、ポリシーベースのバックアップソリューションを備えたフルマネージドバックアップサービスです。このソリューションを使用すると、バックアップの管理が簡素化され、バックアップに関するビジネスおよび規制のコンプライアンス要件を満たすことができます。
2.5A	encrypted-volumes	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化が有効になっていることを確認します。
2.5A	kinesis-stream-encrypted	機密データが含まれている可能性があるため、保管中のデータを保護するために Amazon Kinesis Streams で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
2.5A	s3-bucket-server-side-encryption-enabled	保管中のデータを保護するため、Amazon Simple Storage Service (Amazon S3) バケットで暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、暗号化を有効にしてデータを保護します。
2.5A	s3-default-encryption-kms	Amazon Simple Storage Service (Amazon S3) バケットで、暗号化が有効になっていることを確認します。Amazon S3 バケットには機密データが含まれている可能性があるため、保管中のデータの暗号化を有効にしてデータを保護します。
2.5A	sns-encrypted-kms	保管中のデータを保護するために、Amazon Simple Notification Service (Amazon SNS) トピックで AWS Key Management Service (AWS KMS) を使用した暗号化が必要です。公開されたメッセージには機密データが含まれている可能性があるため、保管時の暗号化を有効にしてデータを保護します。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	iam-password-policy	ID と認証情報は、組織の IAM パスワードポリシーに基づいて発行、管理、検証されます。これらは、NIST SP 800-63 およびパスワード強度に関する AWS Foundational Security Best Practices 標準に記載されている要件を満たしています。このルールでは、オプションで RequireUppercaseCharacters (AWS Foundational Security Best Practices 値： true)、RequireLowercaseCharacters (AWS 基本的なセキュリティのベストプラクティス値： true)、 RequireSymbols (AWS 基礎セキュリティのベストプラクティス値： true)、RequireNumbers (AWS 基礎セキュリティのベストプラクティス値： true)、MinimumPasswordLength (AWS 基礎セキュリティのベストプラクティス値： 14)、PasswordReusePrevention (AWS 基本的なセキュリティのベストプラクティス値： 24)、 および MaxPasswordAge (AWS 基礎セキュリティのベストプラクティス値： 90)。実際の値には、組織のポリシーを反映する必要があります。

コントロール ID	AWS 設定ルール	ガイダンス
4.1	access-keys-rotated	組織のポリシーが指定した通り IAM アクセスキーがローテーションされるようにすることで、認可されたデバイス、ユーザー、プロセスについての認証情報が監査されます。アクセスキーを定期的に変更することが、セキュリティのベストプラクティスです。これにより、アクセスキーがアクティブになっている期間が短縮され、キーが侵害された場合のビジネスへの影響を軽減できます。このルールでは、アクセスキーの更新の値が必要です (Config デフォルト: 90)。実際の値には、組織のポリシーを反映する必要があります。
4.2	iam-user-mfa-enabled	AWS クラウド内のリソースへのアクセスを制限するには、このルールを有効にします。このルールにより、すべてのユーザーの多要素認証 (MFA) が有効になります。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らします。

コントロール ID	AWS 設定ルール	ガイダンス
4.2	mfa-enabled-for-iam-console-access	コンソールパスワードを持つすべての AWS Identity and Access Management (IAM) ユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。MFA は、サインイン認証情報に加えて更なる保護手段を追加します。ユーザーに MFA を要求することで、アカウントが侵害されるインシデントを減らし、権限のないユーザーが機密データにアクセスできないようにすることができます。
4.2	root-account-hardware-mfa-enabled	ルートユーザーに対してハードウェア MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。

コントロール ID	AWS 設定ルール	ガイダンス
4.2	root-account-mfa-enabled	ルートユーザーに対して MFA が有効になっていることを確認して、 AWS クラウド内のリソースへのアクセスを管理します。ルートユーザーは、最も権限のある AWS アカウントのユーザーです。MFA は、サインイン認証情報に更なる保護手段を追加します。ルートユーザーに MFA を要求することで、侵害されるインシデントを減らすことができます AWS アカウント。
5.1	ec2-instance-profile-attached	EC2 インスタンスプロファイルによって、IAM ロールが EC2 インスタンスに渡されます。インスタンスプロファイルをインスタンスにアタッチすることで、最小特権とアクセス許可を管理できます。
5.1	iam-policy-no-statements-with-full-access	IAM アクションが、必要なアクションのみに制限されていることを確認します。タスク完了のために必要以上の権限をユーザーに付与することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
5.1	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することで、システムとアセットへのアクセスを制御できます。root アクセスキーが削除されていることを確認します。代わりに、最小機能の原則を組み込むのに役立つ AWS アカウント ロールベースの を作成して使用します。
5.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) は、ユーザーが少なくとも 1 つのグループのメンバーであることを確認することで、アクセス許可と認可を制限するのに役立ちます。タスク完了のために必要以上の権限をユーザーに許可することは、最小特権と職務の分離の原則に反する可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
5.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) は、指定された期間に使用されていない IAM パスワードとアクセスキーをチェックすることで、アクセス許可と認可に役立ちます。これらの未使用の認証情報が特定された場合は、最小特権の原則に反する可能性があるため、その認証情報を無効にするか、削除する必要があります。このルールでは、maxCredentialUsageAge (Config デフォルト: 90) の値を設定する必要があります。実際の値には、組織のポリシーを反映する必要があります。
5.4	secretsmanager-rotation-enabled-check	このルールにより、 AWS Secrets Manager のシークレットでローテーションが有効になります。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。

コントロール ID	AWS 設定ルール	ガイダンス
5.4	secretsmanager-scheduled-rotation-success-check	このルールにより、 AWS Secrets Manager のシークレットがローテーションスケジュールに従って正常にローテーションされます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。
5.4	secretsmanager-secret-periodic-rotation	このルールにより、 AWS Secrets Manager シークレットで定期的なローテーションが有効になっていることが保証されます。シークレットを定期的にローテーションすることで、シークレットがアクティブになる期間が短縮され、シークレットが侵害された場合のビジネスへの影響が軽減される可能性があります。デフォルト値は 90 日です。

コントロール ID	AWS 設定ルール	ガイダンス
5.4	secretsmanager-using-cmk	保管中のデータを保護するため、 AWS Secrets Manager シークレットで AWS Key Management Service (AWS KMS) による暗号化が有効になっていることを確認します。保管中の Secrets Manager のシークレットに機密データが存在する可能性があるため、保管時の暗号化を有効にしてデータを保護します。
6.4	ec2-instance-detailed-monitoring-enabled	このルールを有効にすると、Amazon EC2 コンソールでの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのモニタリングを改善できます。このルールでは、インスタンスの 1 分ごとのモニタリンググラフが表示されます。
6.4	cloudwatch-log-group-encrypted	保管中の機密データを保護するため、Amazon CloudWatch ロググループで暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
6.4	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch を使用して、イベントのアクティビティログを一元的に収集および管理します。 AWS CloudTrail データを含めると、 内の API コールアクティビティの詳細が提供されます AWS アカウント。
6.4	cloudtrail-enabled	AWS CloudTrail は、 AWS マネジメントコンソールのアクションと API コールを記録することで、否認防止に役立ちます。 AWS サービスを呼び出し AWS アカウント たユーザーと 、呼び出しが生成された送信元 IP アドレス、および呼び出しのタイミングを特定できます。キャプチャされたデータの詳細は、 AWS CloudTrail レコードコンテンツ内に表示されます。
6.4	cloud-trail-encryption-enabled	機密データが存在する可能性があるため、保管中のデータを保護するために、 AWS CloudTrail 証跡で暗号化が有効になっていることを確認します。

コントロール ID	AWS 設定ルール	ガイダンス
6.4	cloud-trail-log-file-validation-enabled	AWS CloudTrail ログファイルの検証を使用して、CloudTrail ログの整合性をチェックします。ログファイルの検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。
6.4	ec2-stopped-instance	このルールを有効にすると、Amazon EC2 インスタンスが、組織の基準に従って許可された日数を超えて停止しているかどうかを確認することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのベースラインの設定を行うことができます。

コントロール ID	AWS 設定ルール	ガイダンス
6.4	vpc-flow-logs-enabled	VPC フローログでは、Amazon Virtual Private Cloud (Amazon VPC) 内のネットワークインターフェイス間で送受信される IP トラフィックに関する情報の詳細な記録を提供します。フローログレコードには、送信元、送信先、プロトコルなど、IP フローのさまざまなコンポーネントの値がデフォルトで含まれています。
6.5A	guardduty-enabled-centralized	Amazon GuardDuty は、脅威インテリジェンスフィードを使用して、潜在的なサイバーセキュリティイベントをモニタリングして検出するのに役立ちます。これには、 AWS クラウド環境内の予期しないアクティビティ、不正なアクティビティ、悪意のあるアクティビティを識別するための悪意のある IPs と機械学習のリストが含まれます。

コントロール ID	AWS 設定ルール	ガイダンス
6.5A	securityhub-enabled	AWS Security Hub は、権限のない担当者、接続、デバイス、ソフトウェアをモニタリングするのに役立ちます。 AWS Security Hub は、複数の AWS サービスからセキュリティアラートや検出結果を集約、整理、優先順位付けします。このようなサービスには、Amazon Security Hub、Amazon Inspector、Amazon Macie、AWS Identity and Access Management (IAM) Access Analyzer、 AWS Firewall Manager、 AWS パートナーソリューションなどがあります。

テンプレート

テンプレートは、GitHub の「SWIFT CSP の運用のベストプラクティス」で入手できます。

Amazon Elastic Container Service (Amazon ECS) のセキュリティのベストプラクティス

このコンフォーマンスパックには、Amazon ECS に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Security Best Practices for Amazon Redshift」(Amazon Redshift のセキュリティベストプラクティス) で入手できます。

Amazon Elastic File System (Amazon EFS) のセキュリティのベストプラクティス

このコンフォーマンスパックには、Amazon EFS に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Security Best Practices for Amazon Redshift」(Amazon Redshift のセキュリティベストプラクティス) で入手できます。

Amazon Elastic Kubernetes Service (Amazon EKS) でのセキュリティに関するベストプラクティス

このコンフォーマンスパックには、Amazon EKS に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Security Best Practices for Amazon EKS」(Amazon EKS のセキュリティベストプラクティス) で入手できます。

Amazon CloudFront のセキュリティのベストプラクティス

このコンフォーマンスパックには、Amazon CloudFront に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Security Best Practices for Amazon Redshift」(Amazon Redshift のセキュリティベストプラクティス) で入手できます。

Amazon OpenSearch Service のセキュリティベストプラクティス

このコンフォーマンスパックには、Amazon OpenSearch Service に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Security Best Practices for Amazon OpenSearch Service」で入手できます。

Amazon Redshift のセキュリティベストプラクティス

このコンフォーマンスパックには、Amazon Redshift に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Security Best Practices for Amazon Redshift」で入手できます。

Amazon Relational Database Service (Amazon RDS) でのセキュリティに関するベストプラクティス

このコンフォーマンスパックには、Amazon RDS に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Security Best Practices for Amazon RDS」(Amazon RDS のセキュリティベストプラクティス) で入手できます。

AWS Auto Scalingのセキュリティのベストプラクティス

このコンフォーマンスパックには、 に基づく AWS Config ルールが含まれています AWS Auto Scaling。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub: Security Best Practices for AWS Auto Scaling で入手できます。

AWS CloudTrailのセキュリティのベストプラクティス

このコンフォーマンスパックには、 に基づく AWS Config ルールが含まれています AWS CloudTrail。でサポートされているすべてのマネージドルールのリストについては AWS Config、「AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub: Security Best Practices for AWS CloudTrail で入手できます。

AWS CodeBuildのセキュリティのベストプラクティス

このコンフォーマンスパックには、 に基づく AWS Config ルールが含まれています AWS CodeBuild。でサポートされているすべてのマネージドルールのリストについては AWS Config、「AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub: Security Best Practices for AWS CodeBuild で入手できます。

Amazon ECR のセキュリティのベストプラクティス

このコンフォーマンスパックには、Amazon Elastic Container Registry (Amazon ECR) に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub の「Security Best Practices for Amazon ECR」 (Amazon RDS のセキュリティベストプラクティス) で入手できます。

AWS Lambdaのセキュリティのベストプラクティス

このコンフォーマンスパックには、 に基づく AWS Config ルールが含まれています AWS Lambda。でサポートされているすべてのマネージドルールのリストについては AWS Config、「AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub: Security Best Practices for AWS Lambda で入手できます。

AWS Network Firewallのセキュリティのベストプラクティス

このコンフォーマンスパックには、 に基づく AWS Config ルールが含まれています AWS Network Firewall。でサポートされているすべてのマネージドルールのリストについては AWS Config、「AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub: Security Best Practices for AWS Network Firewall で入手できます。

Amazon SageMaker AI のセキュリティのベストプラクティス

このコンフォーマンスパックには、Amazon SageMaker AI に基づく AWS Config ルールが含まれています。でサポートされているすべてのマネージドルールのリストについては AWS Config、「AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub のAmazon SageMakerのセキュリティのベストプラクティス」で入手できます。

AWS Secrets Managerのセキュリティのベストプラクティス

このコンフォーマンスパックには、 に基づく AWS Config ルールが含まれています AWS Secrets Manager。でサポートされているすべてのマネージドルールのリストについては AWS Config、「AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub: Security Best Practices for AWS Secrets Manager で入手できます。

AWS WAFのセキュリティのベストプラクティス

このコンフォーマンスパックには、 に基づく AWS Config ルールが含まれています AWS WAF。でサポートされているすべてのマネージドルールのリストについては AWS Config、「 AWS Config マネージドルールのリスト」を参照してください。

必要なパラメータの名前と説明については、次のテンプレートの `Parameters` セクションを参照してください。

テンプレートは、GitHub: Security Best Practices for AWS WAF で入手できます。

修正アクションを含むテンプレートの例

修正をともなう Amazon DynamoDB の運用のベストプラクティス

テンプレートは、GitHub の「Operational Best Practices For Amazon DynamoDB with Remediation」で入手できます。

修正を伴う Amazon S3 の運用のベストプラクティス

テンプレートは、GitHub の「Operational Best Practices For Amazon S3 with Remediation」で入手できます。

テンプレートの構造の詳細については、 AWS CloudFormation ユーザーガイドの「テンプレートの分析」を参照してください。

のカスタムコンフォーマンスパック用のテンプレートの作成 AWS Config

カスタムコンフォーマンスパックは、 アカウントと AWS リージョン、または の組織全体に一緒にデプロイできる AWS Config ルールと修復アクションの一意のコレクションです AWS Organizations。

カスタムコンフォーマンスパックを作成するには、「テンプレートをカスタマイズするセクション」の手順を実行し、使用する AWS Config マネージドルールまたは AWS Config カスタムルールのリストを含む YAML ファイルを作成します。

トピック

- 用語
- テンプレートのカスタマイズ

用語

AWS Config マネージドルールは、 が所有する事前定義されたルールです AWS Config。

AWS Config カスタムルールは、ゼロから作成するルールです。

AWS Config カスタムルールを作成するには、Lambda 関数 (AWS Lambda デベロッパーガイド) と Guard (Guard GitHub リポジトリ) の 2 つの方法があります。これは、 で AWS Lambda 作成された policy-as-code language. AWS Config custom ルールをAWS Config カスタム Lambda ルールと呼び、Guard で作成された AWS Config カスタムルールをAWS Config カスタムポリシールールと呼びます。

テンプレートのカスタマイズ

YAML ファイルの作成

YAML ファイルを作成するには、テキストエディタを開き、ファイルを .yaml として保存します。

> **Note**
>
> ファイルにはパラメータおよびリソースセクションがあります。

パラメータ

YAML ファイルの `Parameters`セクションは、`Resources`セクションの後半で追加する一連のルールの AWS Config ルールパラメータ用です。`Parameters` セクションを作成するには、次のコードブロックをコピーして YAML ファイルに貼り付け、必要に応じてカスタマイズし、ルールパラメータごとに繰り返します。

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

以下に例を示します。

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> カスタムコンフォーマンスパックを構築する AWS Config ルールを選択するときは、 AWS Config ルールに対して評価されるリソースがアカウント内でプロビジョニングされていることを確認します。

1. パラメータセクションの `Parameters:` の 次の行は、*`NameOfRule`* + Param + *`NameOfRuleParameter`* の順序で連結された文字列です。

   a. ルール用に作成した一貫性のある名前を *`NameOfRule`* に置き換えます。たとえば、iam-password-policy ルールには IamPasswordPolicy などと命名することができます。

   b. タイプ `Param`。

   c. 次に、特定のルールのルールパラメータ名を *`NameOfRuleParameter`* に置き換えます。AWS Config マネージドルールの場合、ルールパラメータの名前はマネージドルールのリスト AWS Configにあります (例えば、MinimumPasswordLength は iam-password-policy ルールのルールパラメータの名前です) 。 AWS Config カスタムルールでは、ルールパラメータの名前は、ルールを作成したときに選択した名前です。

2. AWS Config マネージドルールを使用している場合は、マネージド AWS Config ルールのリストで適切なルールを見つけて、`Type`特定のルールの `Default`と の許容値を確認します。 AWS Config カスタムルールでは、ルールを作成するときに選択した値を使用します。

   > **Note**
   >
   > 各パラメータについて、`Type` は必ず指定する必要があります。`Type` は、「String」、「int」、「double」、「CSV」、「boolean」および「StringMap」のいずれかから選択できます。

リソース

Resources セクションには、カスタムコンフォーマンスパックに追加されているルールが一覧表示されます。次の Resources ブロックを Parameters セクションのすぐ下に追加し、必要に応じてカスタマイズし、ルールごとに繰り返します。仕様の詳細については、「AWS::Config::ConfigRule」を参照してください。

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: !Ref NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
        Type: AWS::Config::ConfigRule
     ...
```

以下に例を示します。

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> カスタムコンフォーマンスパックを構築する AWS Config ルールを選択するときは、アカウント内でプロビジョニングされた AWS Config ルールに対して評価されるリソースがあることを確認します。詳細については、[サポートされるリソースタイプ] を参照してください。

1. *NameOfRule* セクションで作成したのと同じ名前に Parameters を置き換えます。

2. AWS Config マネージドルール *ActualConfigRuleName*の場合、 をAWS Config マネージドルールのリストの適切なルールページのタイトルに置き換えます。 AWS Config カスタムルールでは、ルールの作成時に選択した Config ルール名を使用します。
3. `Parameters` セクションで使用したのと同じ名前に *NameOfRuleParameter* を置き換えます。コロンの後に、`Parameters`「」セクションで作成した`!Ref`ものと同じ + *NameOfRule* + Param + *NameOfRuleParameter* の連結文字列をコピーして貼り付けます。
4. *Owner* を適切な値に変更します。

> **Note**
>
> AWS Config マネージドルール
> AWS Config マネージドルールの場合、 の値は `Owner`になります`AWS`。
> AWS Config カスタムルール
> Guard で作成された AWS Config カスタムルールの場合、 の値は `Owner`になります`CUSTOM_POLICY`。Lambda で作成された AWS Config カスタムルールの場合、 の値は `Owner`になります`CUSTOM_LAMBDA`。

5. *SOURCE_IDENTIFIER* を適切な値に変更します。

> **Note**
>
> AWS Config マネージドルール
> AWS Config マネージドルールの場合、AWS Config マネージドルールのリストから選択したルールのリンクに従って識別子をコピーします (たとえば、access-keys-rotated ルールのソース識別子はACCESS_KEYS_ROTATED) 。
> AWS Config カスタムルール
> Lambda で作成された AWS Config カスタムルールの場合、 `SourceIdentifier`はルールの AWS Lambda 関数の Amazon リソースネーム (ARN) です`arn:aws:lambda:us-east-2:123456789012:function:`*ActualConfigRuleName*。Guard で作成された AWS Config カスタムルールの場合、このフィールドは必要ありません。

完全に、塗り分けたカスタムコンフォーマンスパックは、次の AWS Config マネージドルールを使用する例のようになります。iam-password-policy、access-keys-rotated、iam-user-unused-credentials-check。

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: !Ref AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge: !Ref
 IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

のコンフォーマンスパックのデプロイ AWS Config

AWS Config コンソールまたは を使用して AWS CLI 、コンフォーマンスパックをデプロイできます。

Deploy Conformance Packs (Console)

[Conformance packs] (コンフォーマンスパック) ページでは、リージョンのアカウントにコンフォーマンスパックをデプロイできます。また、デプロイされたコンフォーマンスパックを編集および削除することもできます。

AWS Config サンプルテンプレートまたは独自のカスタムテンプレートを使用して、コンフォーマンスパックをデプロイできます。カスタムコンフォーマンスパックの作成方法については、「カスタムコンフォーマンスパック」を参照してください。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. [Conformance packs] (コンフォーマンスパック) ページに移動し、[Deploy conformance pack] (コンフォーマンスパックをデプロイ) を選択します。
3. [Specify template] (テンプレートを指定) ページで、サンプルテンプレートを選択するか、既存のテンプレートを使用します。詳細については、「コンフォーマンスパックサンプルテンプレート」を参照してください。

   - [Use sample template] (サンプルテンプレートを使用) を選択した場合は、サンプルテンプレートのドロップダウンリストから [Sample template] (サンプルテンプレート) を選択します。

     各テンプレートの内容の詳細については、「コンフォーマンスパックのサンプルテンプレート」を参照してください。

   - [Template is ready] (テンプレートの準備ができています) を選択した場合、テンプレートソースを指定します。これは、Amazon S3 URI、 AWS Systems Manager ドキュメント (SSM ドキュメント) 、またはアップロードするテンプレートのいずれかです。

     テンプレートが 50 KB を超える場合は、S3 バケットにアップロードし、その S3 バケットの場所を選択します。例: s3://*bucketname/prefix*。

> **Important**
>
> カスタムコンフォーマンスパックに基づいてコンフォーマンスパックの YAML ファイルをゼロから作成した場合、[Template is ready] (テンプレートの準備ができています) を選択します。

4. [次へ] を選択します。
5. [適合パックの詳細を指定] ページで、適合パックの名前を入力します。

   このコンフォーマンスパック名は、最大 256 文字の英数字を含む一意の名前である必要があります。名前にはハイフンを使用できますが、スペースを含めることはできません。
6. オプション: パラメータを追加します。

   パラメータはテンプレートで定義され、リソースの管理と整理に役立ちます。
7. Next を選択します。
8. [Review and deploy] (レビューとデプロイ) ページで、すべての情報を確認します。

   [Edit] (編集) を選択すると、テンプレートの詳細とコンフォーマンスパックの詳細を編集できます。
9. [Deploy conformance pack] (コンフォーマンスパックをデプロイ) を選択します。

   AWS Config は、コンフォーマンスパックページに適切なステータスでコンフォーマンスパックを表示します。

   コンフォーマンスパックのデプロイに失敗した場合は、アクセス許可を確認し、前提条件のステップを実行したことを確認して、もう一度試してください。または、 にお問い合わせください AWS サポート。

修復を伴うサンプルテンプレートを使用してコンフォーマンスパックをデプロイするには、「A. 修復でコンフォーマンスパックを使用するための前提条件」を参照してから前述の手順を使用してください。

1 つ以上の AWS Config ルールを含むコンフォーマンスパックをデプロイするには、「」を参照してくださいB. 1 つ以上のカスタム AWS Config ルールでコンフォーマンスパックを使用するための前提条件。

Deploy Conformance Packs (AWS CLI)

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. 次のいずれかのコマンドを入力して、**MyConformancePack** という名前の適合パックをデプロイします。テンプレートソースは、Amazon S3 URI、アップロードするテンプレート、または AWS Systems Manager ドキュメント (SSM ドキュメント) のいずれかです。

   Amazon S3 URL

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

   ローカルディレクトリの YAML テンプレート

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   AWS Systems Manager ドキュメント (Systems Manager ドキュメント)

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-ssm-document-details
    DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

3. Enter キーを押してコマンドを実行します。

   次のような出力が表示されます。

   ```
   {
       "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
   MyConformancePack1/conformance-pack-ID"
   }
   ```

> **Note**
>
> コンフォーマンスパック用の YAML テンプレートの作成の詳細については、「カスタムコンフォーマンスパック」を参照してください。

のコンフォーマンスパックの編集 AWS Config

AWS Config コンソールまたは を使用して AWS CLI 、コンフォーマンスパックを編集できます。

Editing Conformance Packs (Console)

1. コンフォーマンスパックを編集するには、テーブルからコンフォーマンスパックを選択します。
2. [Actions] (アクション) を選択して、[Edit] (編集) を選択します。
3. [Edit conformance pack] (コンフォーマンスパックを編集) ページで、テンプレートの詳細、サンプルテンプレート、コンフォーマンスパック、およびパラメータセクションを編集できます。

   コンフォーマンスパックの名前は変更できません。
4. [Save changes] (変更の保存) をクリックします。

   コンフォーマンスパックが AWS Config ルールとともに表示されます。

Editing Conformance Packs (AWS CLI)

以前に追加した適合パックを編集する場合は、適合パックのデプロイ時と同じ `PutConformancePack` コマンドを使用します。

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. 次のいずれかのコマンドを入力して、**`MyConformancePack`** という名前の適合パックをデプロイします。テンプレートソースは、Amazon S3 URI、アップロードするテンプレート、または AWS Systems Manager ドキュメント (SSM ドキュメント) のいずれかです。

   Amazon S3 URL

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   ```

```
--template-s3-uri "s3:///amzn-s3-demo-bucket/templateName.yaml"
--delivery-s3-bucket amzn-s3-demo-bucket
```

ローカルディレクトリの YAML テンプレート

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-body template body
```

AWS Systems Manager ドキュメント (Systems Manager ドキュメント)

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-ssm-document-details
 DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
--delivery-s3-bucket amzn-s3-demo-bucket
```

3. Enter キーを押してコマンドを実行します。

   次のような出力が表示されます。

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> コンフォーマンスパック用の YAML テンプレートの作成の詳細については、「カスタムコンフォーマンスパック」を参照してください。

のコンフォーマンスパックの削除 AWS Config

AWS Config コンソールまたは を使用して AWS CLI 、コンフォーマンスパックを削除できます。

考慮事項

推奨事項: ルールを削除する前に**`AWS::Config::ResourceCompliance`**、リソースタイプを記録から除外することを検討してください。

ルールを削除するCIs) が作成されます。 `AWS::Config::ResourceCompliance`多数のリソースタイプを評価するルールを削除すると、記録された CI の数が増加する可能性があります。

関連するコストを回避するには、ルールを削除する前に`AWS::Config::ResourceCompliance`リソースタイプの記録を無効にし、ルールが削除された後に記録を再度有効にすることができます。

ただし、ルールの削除は非同期プロセスであるため、完了までに 1 時間以上かかる場合があります。の記録が無効になっている間`AWS::Config::ResourceCompliance`、ルール評価は関連するリソースの履歴には記録されません。

コンフォーマンスパックを削除するには

Deleting Conformance Packs (Console)

1. コンフォーマンスパックを削除するには、テーブルからコンフォーマンスパックを選択します。
2. Actions を選択してから、Delete を選択します。
3. ##########の削除ダイアログボックスで、このコンフォーマンスパックを完全に削除するかどうか確認します。

   > **Important**
   >
   > このアクションを元に戻すことはできません。コンフォーマンスパックを削除すると、そのコンフォーマンスパックのすべての AWS Config ルールと修復アクションが削除されます。

4. [Delete] (削除) と入力し、[Delete] (削除) を選択します。

   [Conformance packs] (コンフォーマンスパック) ページでは、コンフォーマンスパックが完全に削除されるまで、デプロイステータスが [Deleting] (削除中) と表示されます。

Deleting Conformance Packs (AWS CLI)

次のコマンドを入力します。

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

成功すると、コマンドは追加の出力なしで実行されます。

> **Important**
>
> このアクションを元に戻すことはできません。コンフォーマンスパックを削除すると、そのコンフォーマンスパックのすべての AWS Config ルールと修復アクションが削除されます。

のコンフォーマンスパックの詳細とコンプライアンス情報の表示 AWS Config

> **Important**
>
> コンプライアンスステータスを正確に報告するには、`AWS::Config::ResourceCompliance` リソースタイプを記録する必要があります。詳細については、AWS 「リソースの記録」を参照してください。

AWS Config コンソールまたは を使用して AWS CLI 、コンフォーマンスパックを表示できます。AWS Config コンソールには統合されたダッシュボードがあります。 AWS CLI では、特定の情報のコマンドを実行できます。

Viewing Conformance Packs (Console)

でコンフォーマンスパックを表示するには AWS Management Console、「コンフォーマンスパックダッシュボードパック」を参照してください。

Viewing the Details for your Conformance Packs (AWS CLI)

1. 次のコマンドを入力します。

   ```
   aws configservice describe-conformance-packs
   ```

   または

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. 次のような出力が表示されます。

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

Viewing the Status for your Conformance Packs (AWS CLI)

1. 次のコマンドを入力します。

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. 次のような出力が表示されます。

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

Viewing the Compliance Status for your Conformance Packs (AWS CLI)

1. 次のコマンドを入力します。

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. 次のような出力が表示されます。

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
        }
    ]
}
```

Viewing the Compliance Details for your Conformance Packs (AWS CLI)

1. 次のコマンドを入力します。

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. 次のような出力が表示されます。

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
```

```
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

のコンフォーマンスパックのコンプライアンス履歴タイムラインの表示 AWS Config

AWS Config は、コンフォーマンスパックへのコンプライアンス状態の変更の保存をサポートします。これにより、コンプライアンスステータスの変更履歴を表示できます。これらのコンプライアンス状態の変更は、タイムラインとして表示されます。タイムラインでは、一定期間の変更を `ConfigurationItems` としてキャプチャします。また、この機能を使ってコンプライアンスパック内にある非準拠の特定のルールを検索できます。

AWS Configのすべてのリソースタイプの記録をオプトインまたはオプトアウトすることができます。すべてのリソースタイプを記録することを選択した場合、 は AWS Config 、ルールによって評価されたコンフォーマンスパックのコンプライアンス履歴 AWS Config の記録を自動的に開始します。デフォルトでは、 はサポートされているすべてのリソースの設定変更 AWS Config を記録します。また、特定のコンフォーマンスパックのコンプライアンス履歴リソースタイプ: `AWS::Config::ConformancePackCompliance` のみを選択することもできます。`AWS::Config::ConformancePackCompliance` リソースタイプの記録は追加料金なしでご利用いただけます。詳細については、AWS 「リソースの記録」を参照してください。

コンフォーマンスパック内のすべてのルールが準拠している場合、コンフォーマンスパックは準拠しています。いずれかのルールが準拠していない場合は、準拠していません。コンフォーマンスパックのコンプライアンスステータスは、データ不足によりコンフォーマンスパック内のすべてのルールを評価できない場合のみ、INSUFFICIENT_DATA になります。コンフォーマンスパック内のルールの一部は準拠しているものの、同じコンフォーマンスパック内の他のルールのコンプライアンスステータスが INSUFFICIENT_DATA である場合、コンフォーマンスパックは準拠と表示されます。適合パックのコンプライアンスは、一度にすべて評価されるわけではありません。ルールによっては、他のルールよりも評価に時間がかかる場合があります。ルールのグループについてコンプライアンスが一度に評価され、コンフォーマンスパック内のすべてのルールが評価されるまで段階的に継続されます。

コンプライアンスのタイムラインの表示

コンプライアンスのタイムラインにアクセスする場合は、[Conformance pack] (コンフォーマンスパック) メインページから特定のコンフォーマンスパックを選択します。

1. [Conformance Pack] (コンフォーマンスパック) ページに移動します。
2. [Conformance Pack] (コンフォーマンスパック) のメインページで、特定のコンフォーマンスパックを選択してから、[Conformance pack timeline] (コンフォーマンスパックのタイムライン) を選択します。

> **Note**
>
> または、コンフォーマンスパックの詳細ページからコンプライアンスタイムラインを使用することもできます。コンフォーマンスパックをクリックし、[Action] (アクション) ドロップダウンで [View details] (詳細を表示) を選択します。このページから、[Conformance pack timeline] (コンフォーマンスパックのタイムライン) を選択します。

タイムラインには、コンフォーマンスパックのコンプライアンスステータスの変更の履歴が表示されます。以下の操作を行うことができます。

1. コンプライアンスの変更を展開して、コンフォーマンスパック内の各ルールのコンプライアンスステータスを行単位で表示します。
2. 展開されたビューから、特定のルールを選択してその詳細ページを表示します。

のコンフォーマンスパックのコンプライアンス履歴のクエリ AWS Config

get-resource-config-history を使用して、リソースタイプ `AWS::Config::ConformancePackCompliance` でコンプライアンス履歴をクエリします。

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

次のような出力が表示されます。

```
{
    "configurationItems": [
        {
            "version": "1.3",
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
```

```
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

詳細については、サポートされているリソースタイプ (AWS Config)および API リファレンスの GetResourceConfigHistory を参照してください。

組織内のすべての AWS Config アカウントにおける のコンフォーマンスパックの管理

を使用して AWS Config 、組織 AWS アカウント 内のすべてのコンフォーマンスパックを管理します。以下の操作を行うことができます。

- AWS Organizationsの組織のメンバーアカウント間でコンフォーマンスパックを一元的にデプロイ、更新、削除します。

- すべてのアカウントに共通の AWS Config ルールと修復アクションのセットをデプロイし、 AWS Config ルールと修復アクションを作成すべきではないアカウントを指定します。
- の 管理アカウントを使用して AWS Organizations 、基盤となる AWS Config ルールと修復アクションが組織のメンバーアカウントによって変更できないようにすることで、ガバナンスを適用します。

考慮事項

異なるリージョンにまたがるデプロイの場合

アカウント間でルールとコンフォーマンスパックをデプロイする API コールは、 AWS リージョン固有です。他のリージョンにルールをデプロイする場合は、組織レベルで API コールのコンテキストを別のリージョンに変更する必要があります。例えば、米国東部 (バージニア北部) にルールをデプロイするには、リージョンを米国東部 (バージニア北部) に変更し、`PutOrganizationConfigRule` を呼び出します。

組織内のアカウントの場合

新しいアカウントが組織に参加すると、ルールまたはコンフォーマンスパックはそのアカウントにデプロイされます。アカウントが組織を離脱すると、そのルールまたはコンフォーマンスパックは削除されます。

組織のルールまたはコンフォーマンスパックを組織管理者アカウントでデプロイし、委任された管理者を確立して、委任された管理者アカウントに組織のルールまたはコンフォーマンスパックをデプロイした場合、委任された管理者アカウントから、組織のルールやコンフォーマンスパックを表示したり、組織の管理者アカウントから、委任された管理者アカウントで組織のルールやコンフォーマンスパックを表示したりすることはできません。DescribeOrganizationConfigRules および DescribeOrganizationConformancePacks API は、これらの API を呼び出すアカウント内からデプロイされた組織関連リソースのみを表示および操作できます。

組織に追加された新しいアカウントに対する再試行メカニズム

レコーダーが利用できない場合、組織の既存のルールと組織のコンフォーマンスパックのデプロイは、アカウントを組織に追加してから 7 時間のみ再試行されます。組織にアカウントを追加してから 7 時間以内にレコーダーが存在しない場合は、レコーダーを作成する必要があります。

組織管理アカウント、委任管理者、サービスにリンクされたロール

組織管理アカウントを使用していて、組織のデプロイに委任管理者を使用する場合、 AWS Config はサービスにリンクされたロール (SLR) を自動的に作成しないことに注意してください。IAM を使用して、サービスにリンクされたロール (SLR) を手動で作成する必要があります。

管理アカウントの SLR がない場合は、委任された管理者アカウントからそのアカウントにリソースをデプロイすることはできません。管理アカウントと委任された管理者アカウントからメンバーアカウントに適合パックをデプロイできます。詳細については、「AWS Identity and Access Management (IAM) ユーザーガイド」の「サービスにリンクされたロールの作成」を参照してください。

デプロイ

To deploy with the AWS Management Console

AWS コンソールから組織全体にコンフォーマンスパックをデプロイするには、 を使用します AWS Systems Manager。詳細については、「 AWS Systems Manager ユーザーガイドAWS Config 」の「適合パックのデプロイ」を参照してください。

To deploy with the AWS API

AWS Config と統合する方法については AWS Organizations、「 AWS Organizations ユーザーガイド」のAWS Config 「」と AWS Organizations「」を参照してください。次の APIs を使用して組織 AWS アカウント 内のすべての でコンフォーマンスパックルールを管理する前に、 AWS Config 録画がオンになっていることを確認します。

- DeleteOrganizationConformancePack は、組織の指定したコンフォーマンスパック、すべての config ルール、および修復アクションをその組織内のすべてのメンバーアカウントから削除します。
- DescribeOrganizationConformancePacks は、組織のコンフォーマンスパックのリストを返します。
- DescribeOrganizationConformancePackStatuses は、組織のコンフォーマンスパックのデプロイステータスを提供します。
- GetOrganizationConformancePackDetailedStatus は、組織の特定のコンフォーマンスパックについて、組織内の各メンバーアカウントの詳細なステータスを返します。
- PutOrganizationConformancePack は、 AWS 組織のメンバーアカウントにコンフォーマンスパックをデプロイします。

リージョンのサポート

Organization のメンバーアカウント間でコンフォーマンスパックをデプロイすることは AWS 、次のリージョンでサポートされています。

リージョン名	リージョン	エンドポイント	プロトコル	
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
米国西部 (北カリフォルニア)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
アジアパシフィック (ハイデラバード)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

のコンフォーマンスパックのトラブルシューティング AWS Config

適合パックを使用する際に発生しうる問題をトラブルシューティングするには、次の問題を確認してください。

トピック

- 適合パックの失敗ステータス
- 適合パック内のダングリングルール

適合パックの失敗ステータス

コンフォーマンスパックの作成、更新、削除中にコンフォーマンスパックが失敗したというエラーが発生した場合は、コンフォーマンスパックのステータスを確認できます。

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

次のような出力が表示されます。

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

ConformancePackStatusReason で失敗に関する情報を確認します。

レスポンスに stackArn が存在する場合

エラーメッセージが明確でない場合、または内部エラーが原因である場合は、 AWS CloudFormation コンソールに移動して次の作業を行います。

1. 出力から stackArn を検索します。
2. CloudFormation スタックの [イベント]タブを選択し、失敗したイベントをチェックします。

   ステータスの理由は、今フォーマンスパックが失敗した理由を示しています。

レスポンスに stackArn が存在しない場合

適合パックの作成中に障害が発生しても、stackArn がステータスレスポンスに存在しない場合、考えられる原因は、スタックの作成に失敗し、CloudFormation がロールバックされ、スタックが削除されていることです。CloudFormation コンソールに移動し、[削除済み] 状態のスタックを検索します。失敗したスタックが見つかる可能性があります。CloudFormation スタックには、適合パック名が含まれます。失敗したスタックが見つかった場合は、CloudFormation スタックの [イベント] タブを選択し、失敗したイベントをチェックします。

これらのどのステップでもうまくいかず、失敗理由が内部サービスエラーである場合は、もう一度オペレーションを試みるか、AWS サポート センターに連絡してください。

適合パック内のダングリングルール

コンフォーマンスパックをデプロイするには、コンフォーマンスパックテンプレートにルールをデプロイするための基盤となる AWS CloudFormation スタックをバックグラウンドで作成する必要があります。これらのルールはサービスにリンクされたルールであり、適合パックの外部で更新または削除することはできません。

基盤となる CloudFormation スタックを変更すると、適合パックとそのルールが管理不能になる状況が発生します。これらの管理不可能なルールはダングリングルールです。

CloudFormation スタックと適合パック間のドリフト

CloudFormation コンソールから直接、適合パックテンプレートのルール名を更新できます。CloudFormation コンソールから直接テンプレートを更新しても、デプロイされた適合パックは更新されません。

このドリフトにより、ダングリングルールが作成されます。適合パックからルールを削除しようとすると、次のようなエラーが発生します。

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

適合パックを削除しようとすると、ダングリングルールを削除できず、次のようなエラーが表示されます。

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

この問題を解決するには、以下の手順を実行します。

1. スタックを削除します。詳細については、CloudFormation ユーザーガイド」のAWS CloudFormation 「コンソールでのスタックの削除」を参照してください。
2. AWS Config コンソールまたは DeleteConformancePack API を使用してコンフォーマンスパックを削除します。組織適合パックで、管理アカウントまたは委任管理者アカウントを使用している場合は、DeleteOrganizationConformancePack API を使用します。
3. 適合パックのダングリングルールの Amazon リソースネーム (ARN) を使用してAWS サポート センターに連絡し、アカウントのクリーンアップに役立ててください。

この問題を回避するには、次のベストプラクティスを覚えておいてください。

- 適合パックの CloudFormation スタックを直接更新しないでください。
- 適合パックとその基盤となる CloudFormation スタックの間にドリフトが生じる変更は絶対に行わないでください。
- 適合パックのサービスリンクロール (SLR) は変更できません。更新するリソースが SLR のアクセス許可ポリシーの一部であることを確認します。

適合パックの削除済み CloudFormation スタック

CloudFormation スタックと適合パックの間にドリフトがない限り、適合パックまたはその CloudFormation スタックのルールを CloudFormation コンソールから直接削除することは推奨されません。

この問題を修正するには、適合パックのダングリングルールの Amazon リソースネーム (ARN) を使用して AWS サポート センターに連絡し、アカウントのクリーンアップに役立ててください。

この問題を回避するには、次のベストプラクティスを覚えておいてください。

- 適合パックの基盤となる CloudFormation スタックは絶対に削除しないでください。
- DeleteConformancePack API を使用して適合パックを削除します。組織適合パックで、管理アカウントまたは委任管理者アカウントを使用している場合は、DeleteOrganizationConformancePack API を使用します。

を使用した非準拠リソースの修復 AWS Config

AWS Config では、 によって評価される非準拠のリソースを修復できます AWS Config ルール。AWS Config は、AWS Systems Manager 自動化ドキュメントを使用して修復を適用します。これらのドキュメントは、 によって評価される非準拠 AWS リソースに対して実行されるアクションを定義します AWS Config ルール。SSM ドキュメントは、 AWS Management Console または API を使用して関連付けることができます。

AWS Config は、修復アクションを含む一連のマネージドオートメーションドキュメントを提供します。カスタムオートメーションドキュメントを作成して AWS Config ルールに関連付けることもできます。

トピック

- リージョンのサポート
- の手動修復のセットアップ AWS Config
- の自動修復の設定 AWS Config
- の修復アクションの削除 AWS Config

リージョンのサポート

現在、 AWS Config ルールの修復アクションは、次のリージョンでサポートされています。

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
米国西部 (北カリ	us-west-1	config.us-west-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
フォルニア)			
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
アジアパシフィック (ハイデラバード)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

の手動修復のセットアップ AWS Config

非準拠のリソースに修復を適用するには、事前入力されたリストから関連付ける修復アクションを選択するか、SSM ドキュメントを使用して独自のカスタム修復アクションを作成します。 は、 で推奨される修復アクションのリスト AWS Config を提供します AWS Management Console。

Setting Up Manual Remediation (Console)

では AWS Management Console、修復アクションを AWS Config ルールに関連付けることで、非準拠のリソースを手動で修復することを選択できます。すべての修復アクションで、手動修復または自動修復のいずれかを選択できます。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. 左側の [Rules] (ルール) を選択後、[Rules] (ルール) ページで [Add Rule] (ルールの追加) を選択して、新しいルールをルールリストに追加します。

   既存のルールの場合は、ルールリストから非準拠のルールを選択後、[Actions] (アクション) を選択します。
3. [アクション] ドロップダウンリストから、[修復の管理] を選択します。[マニュアル修復] を選択後、リストから適切な修復アクションを選択します。

> **Note**
>
> 管理できるのは、サービスにリンクされていない AWS Config ルールの修復のみです。詳細については、「サービスにリンクされた AWS ルール」を参照してください。

選択した修復アクションに応じて、特定のパラメータが表示されるか、パラメータは表示されません。

4. (オプション): 非準拠のリソースのリソース ID を修復アクションに渡す場合は、リソース ID パラメータ を選択します。選択した場合は、そのパラメータは実行時に、修復されるリソースの ID に置き換えられます。

   各パラメータの値は、静的または動的です。ドロップダウンリストから特定のリソース ID パラメータを選択していない場合は、キーごとに値を入力することができます。ドロップダウンリストからリソース ID パラメータを選択した場合は、その他のすべてのキーの値を入力できます (選択したリソース ID のパラメータを除く)。

5. [保存] を選択します。ルール ページが表示されます。

失敗した修復アクションをトラブルシューティングするには、 AWS コマンドラインインターフェイスコマンドを実行して`describe-remediation-execution-status`、一連のリソースの修復実行の詳細ビューを取得できます。詳細には、状態、修復実行ステップのタイムスタンプ、失敗したステップのエラーメッセージが含まれます。

Setting Up Manual Remediation (API)

手動修復を設定するには、次の AWS Config API オペレーションを使用します。

- PutRemediationConfigurations は、選択したターゲットまたはアクションを持つ特定の AWS Config ルールで修復設定を追加または更新します。
- StartRemediationExecution は、最後の既知の修復設定に対して、指定された AWS Config ルールのオンデマンド修復を実行します。
- DescribeRemediationExecutionStatus は、一連のリソースに対する修復実行の詳細ビュー (状態、修復実行のステップが発生する時点のタイムスタンプ、失敗したステップのエラーメッセージなど) を提供します。
- DescribeRemediationConfigurations は、1 つ以上の修復設定の詳細を返します。

の自動修復の設定 AWS Config

非準拠のリソースに修復を適用するには、事前入力されたリストから関連付ける修復アクションを選択するか、SSM ドキュメントを使用して独自のカスタム修復アクションを作成します。 は、 で修復アクションのリスト AWS Config を提供します AWS Management Console。

Setting Up Auto Remediation (Console)

では AWS Management Console、修復アクションを AWS Config ルールに関連付けることで、非準拠のリソースを自動的に修復することを選択できます。すべての修復アクションで、手動修復または自動修復のいずれかを選択できます。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. 左側の [ルール] を選択後、[ルール] ページで [ルールの追加] を選択して、新しいルールをルールリストに追加します。

   既存のルールの場合は、ルールリストから非準拠のルールを選択後、[Actions] (アクション) を選択します。
3. [アクション] ドロップダウンリストから、[修復の管理] を選択します。「自動修復」を選択し、リストから適切な修復アクションを選択します。

   > **Note**
   > 管理できるのは、サービスにリンクされていない AWS Config ルールの修復のみです。詳細については、「サービスにリンクされた AWS ルール」を参照してください。

   選択した修復アクションに応じて、特定のパラメータが表示されるか、パラメータは表示されません。
4. [Auto remediation] (自動修復) を選択して、非準拠のリソースを自動的に修復します。

   自動修復後もリソースがまだ非準拠である場合は、自動修復を再試行するようにルールを設定できます。目的の再試行階数と秒数を入力します。

> **Note**
>
> 修復スクリプトを複数回実行するとコストがかかります。修復が失敗し、指定された期間内に処理が行われた場合にのみ再試行を実行します。例えば、300 秒に 5 回再試行します。詳細については、「Systems Manager Automation の料金」を参照してください。

5. (オプション): 非準拠のリソースのリソース ID を修復アクションに渡す場合は、リソース ID パラメータ を選択します。選択した場合は、そのパラメータは実行時に、修復されるリソースの ID に置き換えられます。

   各パラメータの値は、静的または動的です。ドロップダウンリストから特定のリソース ID パラメータを選択していない場合は、キーごとに値を入力することができます。ドロップダウンリストからリソース ID パラメータを選択した場合は、その他のすべてのキーの値を入力できます (選択したリソース ID のパラメータを除く)。

6. [保存] を選択します。ルール ページが表示されます。

失敗した修復アクションのトラブルシューティング

失敗した修復アクションをトラブルシューティングするには、 AWS コマンドラインインターフェイスコマンドを実行して`describe-remediation-execution-status`、一連のリソースの修復実行の詳細ビューを取得できます。詳細には、状態、修復実行ステップのタイムスタンプ、失敗したステップのエラーメッセージが含まれます。

準拠しているリソースでも自動修復を開始できます

PutRemediationConfigurations API または AWS Config コンソールを使用して特定の AWS Config ルールの自動修復を有効にすると、その特定のルールのすべての非準拠リソースの修復プロセスが開始されます。自動修復プロセスは、定期的にキャプチャされるコンプライアンスデータスナップショットに依存します。スナップショットスケジュール間で更新された非準拠リソースは、最後に確認されたコンプライアンスデータスナップショットに基づいて引き続き修正されます。

つまり、ブートストラッププロセッサは、最後に既知のコンプライアンスデータスナップショットに基づいて古い評価結果を持つデータベースを使用するため、場合によっては、準拠しているリソースであっても自動修復を開始できます。

Setting Up Auto Remediation (API)

自動修復を設定するには、次の AWS Config API オペレーションを使用します。

- PutRemediationExceptions は、新しい例外を追加するか、特定の AWS Config ルールを持つ特定のリソースの既存の例外を更新します。
- DescribeRemediationExceptions は、1 つ以上の修復例外の詳細を返します。

の修復アクションの削除 AWS Config

AWS Config コンソールまたは を使用して AWS CLI 、修復アクションを削除できます。

Deleting remediation actions (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. 左側から [Rules] (ルール) を選択したら、[Rules] (ルール) ページでルールのリストからルールを選び、[View details](詳細を表示) を選択します。
3. リポジトリの *[name of the rule]* (ルールの名前) ページで、[Remediation action] (修復アクション) セクションに追加します。セクションを展開し、追加の詳細を表示します。
4. [Remediation action] (修復アクション) セクションで、[Delete] (削除) をクリックし、削除アクションを確認します。

> **Note**
>
> 修復が進行中の場合には、修復アクションは削除されません。Delete remediation action (修復アクションの削除) を選択すると、修復アクションを回復することはできません。修復アクションを削除しても、関連付けられたルールは削除されません。

修復アクションが削除されると、[Resource ID parameter] (リソース ID パラメータ) は空になり、N/A と表示されます。[Rules] (ルール) ページで、修復アクション列に関連付けられたルールに対して [Not set] (設定されていません) と表示されます。

Deleting remediation actions (API)

自動修復を設定するには、次の AWS Config API オペレーションを使用します。

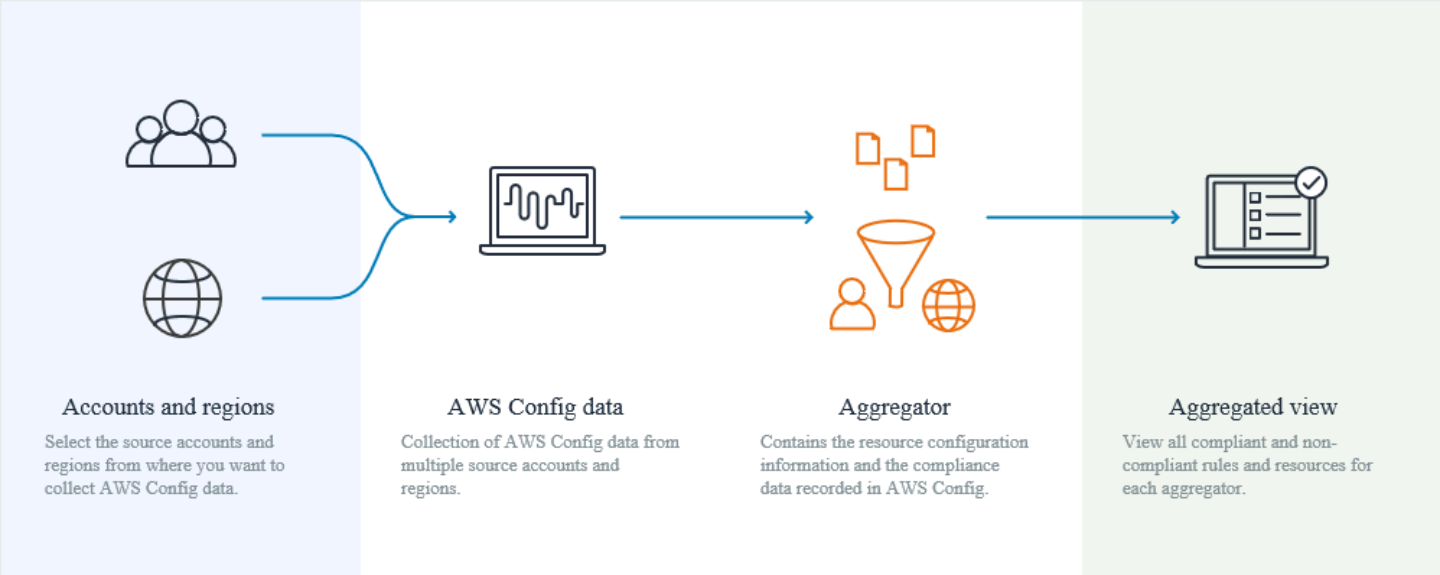
- DeleteRemediationConfiguration は、修復設定を削除します。
- DeleteRemediationExceptions は、リソースキーに記載されている 1 つ以上の修復例外を削除します。

のマルチアカウントマルチリージョンデータ集約 AWS Config

アグリゲータは、以下から AWS Config 設定およびコンプライアンスデータを収集する AWS Config リソースタイプです。

- 複数のアカウントと複数の AWS リージョン。
- 1 つのアカウントと複数の AWS リージョン。
- の組織 AWS Organizations と、その組織で AWS Config が有効になっているすべてのアカウント。

リソース設定と、 AWS Configに記録されたコンプライアンスデータを表示するには、アグリゲータを使用します。次の図は、アグリゲータが複数のアカウントとリージョンから AWS Config データを収集する方法を示しています。



ユースケース

- コンプライアンスモニタリング: コンプライアンスデータを集約して、組織の全体的なコンプライアンス体制、またはアカウントとリージョン全体で評価できます。
- 変更追跡: 組織全体、またはアカウントとリージョン間で、リソースへの変更を経時的に追跡できます。

- リソース関係 : 組織全体、またはアカウントとリージョン間でリソースの依存関係と関係を分析できます。

> **Note**
>
> アグリゲータでは、ソースアカウントからアグリゲータアカウントにデータをレプリケートすることにより、アグリゲータが閲覧を許可されているソースアカウントとリージョンに対して、読み取り専用ビューを提供します。アグリゲータでは、ソースアカウントまたはリージョンへの変更アクセスを提供しません。例えば、アグリゲータを使用してルールをデプロイしたり、アグリゲータを介してソースアカウントまたはリージョンにスナップショットファイルをプッシュしたりできないということを意味します。
> アグリゲータを使用しても、追加コストは発生しません。

用語

ソースアカウントは、 AWS Config リソース設定とコンプライアンスデータを集約する AWS アカウント です。ソースアカウントは、個別のアカウントまたは AWS Organizationsの組織を指定できます。ソースアカウントは個別に提供することも、取得することもできます AWS Organizations。

ソースリージョンは、 AWS Config 設定データとコンプライアンスデータを集約する AWS リージョンです。

アグリゲータアカウントは、アグリゲータを作成するアカウントです。

認可とは、 AWS Config 設定とコンプライアンスデータを収集するためにアグリゲータアカウントとリージョンに付与するアクセス許可を指します。 AWS Organizationsの一部であるソースアカウントを集約する場合、承認は必要ありません。

サービスにリンクされたアグリゲータは、特定の にリンクされます AWS のサービス。範囲内の設定データとコンプライアンスデータは、リンクされたサービスによって設定されます。

リージョンのサポート

現在、マルチアカウントマルチリージョンのデータ集約は次のリージョンでサポートされています。

リージョン名	リージョン	エンドポイント	プロトコル	
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
米国西部 (北カリフォルニア)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
アジアパシフィック (ハイデラバード)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (マレーシア)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (台北)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
アジアパシフィック (タイ)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
メキシコ (中部)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル	
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS	

のアグリゲータダッシュボードでのコンプライアンスデータとインベントリデータの表示 AWS Config

アグリゲータページのダッシュボードには、集約された AWS リソースの設定データが表示されます。ルール、適合パック、およびコンプライアンスの状態の概要が示されます。

ダッシュボードには、リソースの合計 AWS リソース数が表示されます。リソースタイプとソースアカウントは、リソースの最大数によってランク付けされます。準拠ルール、非準拠ルール、および適合パックの数も表示されます。非準拠ルールは、非準拠リソースの最大数によってランク付けされます。非準拠適合パックとソースアカウントは、非準拠ルールの最大数によってランク付けされます。

設定後 AWS Config、指定されたソースアカウントからアグリゲータへのデータの集約が開始されます。ルールのコンプライアンス状態を表示するまでに、数分かかる場合があります。

アグリゲータダッシュボードの使用

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. [アグリゲータ] ページに移動します。 次を表示できます。
   - ルールとそのコンプライアンス状態。
   - 適合パックとそのコンプライアンス状態。
   - AWS リソースとその設定データ。
3. ダッシュボードで [アグリゲータ] を選択します。アグリゲータ名でアグリゲータをフィルタリングします。次のウィジェットを表示できます。
   - リソースインベントリ

選択したアグリゲータから上位 10 のリソースタイプを、リソース数の降順で表示します。[リソースのインベントリ] の後の括弧内に表示される、選択したアグリゲータのリソースの総数を選択すると、集約された [リソース] ページに移動します。このページでは、アグリゲータのすべてのリソースを表示できます。または、ウィジェットでリソースタイプを選択すると、集約された [リソース] ページに移動します。このページは、指定したリソースタイプを使用してフィルタリングされています。

- リソース数別アカウント

  選択したアグリゲータから上位 5 つのアカウントを、リソース数の降順で表示します。ウィジェットでアカウントを選択すると、指定したアカウントを使用してフィルタリングされた [リソース] ページに移動します。

- 非準拠ルール

  選択したアグリゲータの上位 5 つの非準拠ルールを、非準拠リソースの数の降順で表示します。ウィジェットのルールを選択すると、指定したルールの [詳細] ページに移動します。[すべての非準拠ルールを表示] を選択すると、集約された [ルール] ページに移動し、アグリゲータのすべてのルールを表示できます。

- 非準拠ルール別アカウント

  選択したアグリゲータから上位 5 つのアカウントを、非準拠ルール数の降順で表示します。ウィジェットでアカウントを選択すると、集約された [ルール] ページに移動し、指定したアカウントを使用してフィルタリングされたアグリゲータのすべてのルールを表示できます。

- 準拠していない準拠パック別アカウント

  選択したアグリゲータから上位 5 つのアカウントを、非準拠パック数の降順で表示します。ウィジェットでアカウントを選択すると、集約された [適合パック] ページに移動し、指定したアカウントを使用してフィルタリングされたアグリゲータのすべての適合パックを表示できます。

4. 左側のナビゲーションペインで、ドロップダウンメニューから次のオプションの 1 つを選択します。

   - コンプライアンスダッシュボード

     アグリゲータ内のリソースコンプライアンスに関するインサイトを要約するウィジェットを使用して、自動コンプライアンスダッシュボードを表示できます。非準拠リソース別の上位 10 のリソースタイプや、非準拠ルール別のアカウントレベルの上位 10 の適合パックなどのデー

タを表示できます。これらのグラフやチャートについては、「コンプライアンスダッシュボード」を参照してください。

- 適合パック

  アグリゲータ AWS アカウント 内で作成され、異なる にリンクされているすべてのコンフォーマンスパックを表示します。[適合パック] ページには、各適合パックの名前、リージョン、アカウント ID、およびコンプライアンスステータスを一覧表示するテーブルが表示されます。このページから、適合パックと [詳細を表示] をクリックすると、ルールとリソース、およびコンプライアンスステータスの詳細を確認できます。

- ルール

  アグリゲータ内で作成され、異なる AWS アカウントにリンクされているルールをすべて表示します。[ルール] ページには、各ルールの名前、コンプライアンスステータス、リージョン、アカウントの一覧表が表示されます。このページから、ルールと [詳細を表示] をクリックすると、アグリゲータ、リージョン、アカウント ID、スコープ内のリソースなどの情報を確認できます。

- インベントリダッシュボード

  アグリゲータ内のリソース設定データに関するインサイトを要約するウィジェットを使用して、自動インベントリダッシュボードを表示できます。リソース数別の上位 10 のリソースタイプや、リソース数別の上位 10 のアカウントなどのデータを表示できます。これらのグラフやチャートについては、「インベントリダッシュボード」を参照してください。

- リソース

  アグリゲータ内で記録され、異なる AWS アカウントにリンクされているリソースをすべて表示します。[リソース] ページで、リソースと [詳細を表示] を選択して、詳細とそれに関連付けられたルール、および現在のリソース設定を表示します。また、アグリゲータ、リージョン、アカウント ID、リソース名、リソースタイプ、リソース ID など、リソースに関する情報を表示することもできます。

- 認証

  現在承認されている、または承認が保留中のアカウントをすべて表示し、管理します。[認証] ページから、[承認の追加] を選択して、別のアカウントへのアクセスを許可します。アカウント ID からアクセスを取り消すには [認証の削除] を選択します。

> **Note**
>
> トラブルシューティング
> 次の理由により、すべてのソースアカウントとリージョンからのデータ収集が不完全なメッセージが集計ビューに表示されることがあります。
>
> - AWS リソースの非準拠 AWS Config ルールと設定データの転送が進行中です。
> - AWS Config は、適用したフィルターに一致するルールを見つけることができません。適切なアカウントまたはリージョンを選択して、もう一度試してください。
>
> このメッセージが集約ビューに表示される場合があります。組織からのデータ収集が不完全です。以下のデータは 24 時間だけ表示できます。これは、次のような理由で表示されます。
>
> - AWS Config 有効でない IAM ロールのため、 は組織の詳細にアクセスできません。IAM ロールが 24 時間以上は無効である場合、 AWS Config は組織全体のデータを削除します。
> - AWS Config サービスアクセスは組織内で無効になっています。

コンプライアンスダッシュボード

アグリゲータ内のリソースコンプライアンスに関するインサイトを要約するウィジェットを使用して、自動コンプライアンスダッシュボードを表示できます。このダッシュボードはコンプライアンス結果のあるルールだけを表示します。

> **Note**
>
> 制約事項
> コンプライアンスダッシュボードのインサイトは、 の高度なクエリ機能によって提供され AWS Config、この機能はネストされた構造やネストされた配列の解凍をサポートしていません。つまり、コンプライアンスダッシュボードには、リソースの全体的なコンプライアンスが表示され、リソースについてレポートする特定のルールごとのコンプライアンスステータスは表示されません。
> 例えば、リソースタイプ `AWS::Config::ResourceCompliance` の設定項目 (CI) をチェックすると、ダッシュボードには、そのリソースについてレポートするすべてのルールのコンプライアンス結果が表示されます。リソースについてレポートするルールが 10 個あり、そ

のうち 9 個が COMPLIANT、1 個のみが NON_COMPLIANT の場合、そのリソースの全体的なコンプライアンスは NON_COMPLIANT になります。

コンプライアンスの概要 (リソース別)

選択したアグリゲータから準拠リソースと非準拠リソースの数を比較した円グラフを表示します。グラフの上にカーソルを移動すると、準拠リソースと非準拠リソースの正確な数と割合が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。

非準拠リソース別の上位 10 のリソースタイプ

選択したアグリゲータから最大 10 のリソースタイプを、水平方向の棒グラフで、非準拠リソース数の降順で表示します。グラフの上にカーソルを移動すると、各リソースタイプの非準拠リソースの正確な数が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。

非準拠リソース別の上位 10 のアカウント

非準拠リソース別の上位 10 のアカウントには、選択したアグリゲータから最大 10 のアカウントが、水平方向の棒グラフで、非準拠リソース数の降順で表示します。グラフの上にカーソルを移動すると、各アカウントの非準拠リソースの正確な数が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。

非準拠リソース別の上位 10 のリージョン

選択したアグリゲータがデータを収集するリージョンを最大 10 比較する水平方向の棒グラフを、非準拠リソース数の降順で表示します。グラフの上にカーソルを移動すると、各リージョンの非準拠リソースの正確な数が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定よって異なります。

非準拠ルール別の上位 10 のアカウントレベルの適合パック

選択したアグリゲータから最大 10 のアカウントレベルの適合パックを、水平方向の棒グラフで、非準拠ルール数の降順で表示します。グラフの上にカーソルを移動すると、各アカウントレベルの適合パックの準拠ルールと非準拠ルールの割合が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。

非準拠ルール別の上位 10 の組織レベルの適合パック

選択したアグリゲータから最大 10 の組織レベルの適合パックを、水平方向の棒グラフで、非準拠ルール数の降順で表示します。グラフの上にカーソルを移動すると、各組織レベルの適合パックの準拠ルールと非準拠ルールの割合が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。

適合パック間の非準拠ルール別の上位 10 のアカウント

適合パック間の非準拠ルール別の上位 10 のアカウントには、選択したアグリゲータから最大 10 のアカウントが、水平方向の棒グラフで、適合パック間の非準拠リソース数の降順で表示されます。グラフの上にカーソルを移動すると、各アカウントの非準拠ルールの正確な数が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。

インベントリダッシュボード

アグリゲータ内のリソース設定データに関するインサイトを要約するウィジェットを使用して、自動インベントリダッシュボードを表示できます。

リソース数別の上位 10 のリソースタイプ

選択したアグリゲータから最大 10 のリソースタイプを、水平方向の棒グラフで、リソース数の降順で表示します。グラフの上にカーソルを移動すると、各リソースタイプのリソースの正確な数が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。

リソース数 (リージョン別)

選択したアグリゲータがデータを収集するリージョンを最大 10 比較する水平方向の棒グラフを、リソース数の降順で表示します。グラフの上にカーソルを移動すると、各リージョンのリソースの正確な数が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定よって異なります。

リソース数別の上位 10 のアカウント

選択したアグリゲータから最大 10 のアカウントを、水平方向の棒グラフで、リソース数の降順で表示します。グラフの上にカーソルを移動すると、各リソースタイプの正確なリソースの数が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。

Amazon EC2 サービスのリソースタイプ別のリソース数

選択したアグリゲータから Amazon EC2 のリソースタイプを比較する水平方向の棒グラフが、リソース数の降順で表示されます。グラフの上にカーソルを移動すると、各 Amazon EC2 リソースタイプの正確なリソース数が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。このグラフを使用するには、Amazon EC2 リソースタイプを記録するようにレコーダーを設定する必要があります。詳細については、AWS Config 「記録するリソースの選択」を参照してください。

使用されている上位 10 の EC2 インスタンスタイプ

選択したアグリゲータから最大 10 の Amazon EC2 インスタンスタイプを比較する水平方向の棒グラフが、使用状況の降順で表示されます。グラフの上にカーソルを移動すると、各 EC2 インスタンスタイプの使用状況が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。このグラフを使用するには、EC2 インスタンスのリソースタイプを記録するようにレコーダーを設定する必要があります。詳細については、AWS 「リソースのコーディング」を参照してください。

ボリュームタイプとサイズ別の EBS ボリューム数

選択したアグリゲータから EBS ボリュームをリソース数別に比較した垂直方向の棒グラフを表示します。グラフの上にカーソルを移動すると、各 EBS ボリュームのタイプの数とサイズの内訳が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。このグラフを使用するには、EC2 ボリュームのリソースタイプを記録するようにレコーダーを設定する必要があります。詳細については、AWS Config 「記録するリソースの選択」を参照してください。

実行中および停止中の EC2 インスタンスの数 (タイプ別)

選択したアグリゲータから実行中の EC2 インスタンスタイプと停止している EC2 インスタンスをインスタンスタイプ別に比較した水平方向の棒グラフを表示します。グラフの上にカーソルを移動すると、各タイプの停止中および実行中の EC2 インスタンスの正確な数が表示されます。

表示されるデータは、選択したアグリゲータの各アカウントの設定レコーダーの設定と、選択したアグリゲータがデータを収集するように設定されているリージョンによって異なります。このグラフを使用するには、EC2 インスタンスのリソースタイプを記録するようにレコーダーを設定する必要があります。詳細については、AWS 「リソースのコーディング」を参照してください。

のアグリゲータの作成 AWS Config

AWS Config コンソールまたは AWS CLI を使用して、アグリゲータを作成できます。から AWS Config 、個々のアカウント IDs を追加するか、データを集約する組織を追加するかを選択できます。には 2 つの異なる手順 AWS CLI があります。

Creating Aggregators (Console)

[アグリゲータ] ページで、データを集約するソースアカウント ID または組織とリージョンを指定して、アグリゲータを作成することができます。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. [アグリゲータ] ページに移動し、[アグリゲータの作成] をクリックします。
3. [データのレプリケーションを許可] では、ソースアカウントからアグリゲータアカウントにデータをレプリケートするアクセス許可を AWS Config に付与します。

ソースアカウント (複数可) からアグリゲータアカウントにデータをレプリケート AWS Config することを許可するを選択します。続行してアグリゲータを追加するには、このチェックボックスをオンにする必要があります。

4. [アグリゲータ名] に、アグリゲータの名前を入力します。

   このアグリゲータ名は、最大 64 文字の英数字を含む一意の名前である必要があります。この名前には、ハイフンとアンダースコアを使用できます。

5. [ソースアカウントの選択] で、データの集約元となる [個々のアカウント ID を追加する] または [組織の追加] を選択します。

> **Note**
>
> [個々のアカウント ID を追加する] を使用してソースアカウントを選択する場合は、認可が必要です。

- [個々のアカウント ID を追加する] を選択した場合は、アグリゲータアカウントの個別のアカウント ID を追加できます。
  1. アカウント ID を追加するには、[ソースアカウントの追加] を選択します。
  2. Add AWS アカウント IDs を選択して、カンマ区切り AWS アカウント IDs。現在のアカウントからデータを集約する場合は、アカウントのアカウント ID を入力します。

     または

     [ファイルのアップロード] をクリックして、カンマで区切られた AWS アカウント ID のファイル (.txt または .csv) をアップロードします。
  3. [ソースアカウントの追加] を選択して、選択を確定します。
- [組織の追加] を選択した場合、組織のすべてのアカウントをアグリゲータアカウントに追加することができます。

> **Note**
>
> 管理アカウントまたは登録済みの委任された管理者にサインインしていて、組織のすべての機能が有効になっている必要があります。発信者が管理アカウントの場合、 は `EnableAwsServiceAccess` API を AWS Config 呼び出して AWS Config と の統合を有効にします AWS Organizations。発信者が登録済みの委任管理者で

ある場合、 は `ListDelegatedAdministrators` API を AWS Config 呼び出して、発信者が有効な委任管理者かどうかを確認します。
委任管理者がアグリゲータを作成する前に、管理アカウントが AWS Config サービスプリンシパル名 (config.amazonaws.com) の委任管理者を登録していることを確認します。委任された管理者を登録するには、「の委任管理者の登録 AWS Config」を参照してください。

が組織の読み取り専用 APIs AWS Config を呼び出すには、IAM ロールを割り当てる必要があります。

1. [アカウントからロールを選択] をクリックして、既存の IAM ロールを選択します。

> **Note**
>
> IAM コンソールで、`AWSConfigRoleForOrganizations` 管理ポリシーを IAM ロールにアタッチします。このポリシーをアタッチすると、 は `DescribeOrganization`、`ListAWSServiceAccessForOrganization`、および `ListAccounts` API AWS Config を呼び AWS Organizations 出すことができます。 APIs デフォルトでは、`config.amazonaws.com` が信頼された エンティティとして自動的に指定されます。

2. または、[ロールを作成する] を選択して、IAM ロール名の名前を入力し、IAM ロールを作成します。

6. [リージョン] で、データを集約するリージョンを選択します。
   - 1 つのリージョン、複数のリージョン、またはすべての AWS リージョンリージョンを選択します。
   - 「未来を含める AWS リージョン」を選択して、マルチアカウントのマルチリージョンデータ集約が有効になってい AWS リージョン るすべての未来のデータを集約します。
7. Save. AWS Config displays を選択します。

Creating Aggregators using Individual Accounts (AWS CLI)

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. 次のコマンドを入力して、**`MyAggregator`** という名前のアグリゲータを作成します。

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

`account-aggregation-sources` については、次のいずれかを入力します。

- データを集約する AWS アカウント IDs のカンマ区切りリスト。アカウント ID を角括弧で囲み、必ず疑問符をエスケープします (例: `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`)。
- カンマ区切りの AWS アカウント ID の JSON ファイルをアップロードすることもできます。次の構文を使用して、ファイルをアップロードします。`--account-aggregation-sources MyFilePath/MyFile.json`

  JSON ファイルの形式は、次のようになります。

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. Enter キーを選択して、コマンドを実行します。

   次のような出力が表示されます:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
```

```
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Creating Aggregators using AWS Organizations (AWS CLI)

この手順を開始する前に、管理アカウントまたは登録済みの委任された管理者にサインインしていて、すべての機能が組織で有効になっている必要があります。

> **Note**
>
> 委任管理者がアグリゲータを作成する前に、管理アカウントが次の AWS Config サービスプリンシパル名 (`config.amazonaws.com` と `config-multiaccountsetup.amazonaws.com`) の両方を持つ委任管理者を登録していることを確認します。委任された管理者を登録するには、の委任管理者の登録 AWS Config を参照してください。

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. アグリゲータの IAM AWS Config ロールを作成していない場合は、次のコマンドを入力します。

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> アグリゲータの作成時に使用するために、この IAM ロールから Amazon リソースネーム (ARN) AWS Config をコピーします。ARN はレスポンスオブジェクト内にあります。

3. IAM ロールにポリシーをアタッチしていない場合は、AWSConfigRoleForOrganizations マネージドポリシーをアタッチするか、次のコマンドを入力します。

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAw
```

4. 次のコマンドを入力して、**MyAggregator** という名前のアグリゲータを作成します。

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. Enter キーを選択して、コマンドを実行します。

   次のような出力が表示されます:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

の委任管理者の登録 AWS Config

委任された管理者は、指定された AWS サービスに追加の管理者権限が付与された、特定の AWS 組織内のアカウントです。詳細については、「AWS Organizations ユーザーガイド」の「委任された管理者」を参照してください。 AWS CLI を使用して委任管理者を登録できます。

委任管理者の登録

1. 管理アカウントの認証情報を使用してログインします。
2. コマンドプロンプトまたはターミナルウィンドウを開きます。
3. 次のコマンドを入力して、組織の委任管理者としてサービスアクセスを有効にし、組織全体に AWS Config ルールとコンフォーマンスパックをデプロイおよび管理します。

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. 次のコマンドを入力して、組織の委任管理者としてサービスアクセスを有効にし、組織全体の AWS Config データを集約します。

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. サービスアクセスの有効化が完了したかどうかを確認するには、次のコマンドを入力し、Enter キーを押してコマンドを実行します。

```
aws organizations list-aws-service-access-for-organization
```

次のような出力が表示されます:

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
    ]
```

```
}
```

6. 次に、次のコマンドを入力して、メンバーアカウントを AWS Configの委任された管理者として登録します。

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

and

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. 委任された管理者の登録が完了したかどうかを確認するには、管理アカウントから次のコマンドを入力し、Enter キーを押してコマンドを実行します。

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

and

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

次のような出力が表示されます:

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::ManagementAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
```

```
}
```

のアグリゲータの編集 AWS Config

AWS Config コンソールまたは AWS CLI を使用して、アグリゲータを編集できます。

Editing Aggregators (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. [アグリゲータ] ページに移動し、アグリゲータ名を選択します。
3. [アクション] を選択して、[編集] を選択します。
4. [アグリゲータの編集] ページのセクションを使用して、アグリゲータのソースアカウント、IAM ロール、またはリージョンを変更します。

   > **Note**
   >
   > 個別のアカウントから組織に、またはその逆にソースタイプを変更することはできません。

5. [保存] を選択します。

Editing Aggregators (AWS CLI)

1. 設定アグリゲータを更新または編集するには、`put-configuration-aggregator` コマンドを使用できます。

   次のコマンドを入力して、新しいアカウント ID を **`MyAggregator`** に追加します。

   ```
   aws configservice put-configuration-aggregator --configuration-aggregator-name
    MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
   \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
   ```

2. ソースアカウントに応じて、次のような出力が表示されます。

   個別のアカウントの場合

   ```
   {
   ```

```
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

または

組織の場合

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

のアグリゲータの削除 AWS Config

AWS Config コンソールまたは AWS CLI を使用して、アグリゲータを削除できます。

Deleting Aggregators (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. [アグリゲータ] ページに移動し、アグリゲータ名を選択します。
3. [アクション] を選択してから、[削除] を選択します。

   警告メッセージが表示されます。アグリゲータを削除すると、すべての集約されたデータが失われます。このデータは復元できませんが、ソースアカウントのデータへの影響はありません。
4. [削除] を選択して、選択を確定します。

Deleting Aggregators (AWS CLI)

次のコマンドを入力します。

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

成功すると、コマンドは追加の出力なしで実行されます。

アグリゲータアカウントで AWS Config 設定とコンプライアンスデータの収集を承認する

認可とは、 AWS Config 設定とコンプライアンスデータを収集するためにアグリゲータアカウントとリージョンに付与するアクセス許可を指します。 AWS Organizationsの一部であるソースアカウントを集約する場合、承認は必要ありません。 AWS Config コンソールまたは を使用して、アグリゲータアカウント AWS CLI を承認できます。

トピック

- 考慮事項
- 認証の追加

考慮事項

アグリゲータには、個別アカウントアグリゲータと組織アグリゲータの 2 種類があります

個人アカウントアグリゲータの場合、外部アカウントとリージョン、組織のメンバーアカウントとリージョンの両方を含め、希望するすべてのソースアカウントとリージョンの承認が必要です。

組織アグリゲータの場合、認可は AWS Organizations サービスと統合されているため、組織メンバーアカウントリージョンに認可は必要ありません。

アグリゲータ AWS Config はユーザーに代わって を自動的に有効にしません

AWS Config ソースアカウントとリージョンで AWS Config データを生成するには、いずれかのタイプのアグリゲータのソースアカウントとリージョンで を有効にする必要があります。

認証の追加

Adding Authorization (Console)

アグリゲータアカウントとリージョンに、 AWS Config 設定とコンプライアンスデータを収集するアクセス許可を付与する認可を追加できます。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. [認証] ページに移動し、[承認の追加] を選択します。
3. [アグリゲータアカウント] に、アグリゲータアカウントの 12 桁のアカウント ID を入力します。
4. [アグリゲータのリージョン] で、アグリゲータアカウントが AWS Config 設定とコンプライアンスデータの収集を許可される AWS リージョン を選択します。
5. [承認の追加] を選択して、選択を確定します。

   AWS Config は、アグリゲータアカウント、リージョン、認可ステータスを表示します。

   > **Note**
   >
   > AWS CloudFormation サンプルテンプレートを使用して、プログラムでアグリゲータアカウントとリージョンに認可を追加することもできます。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS::Config::AggregationAuthorization」を参照してください。

Authorizing a Pending Request (Console)

既存のアグリゲータアカウントからの保留中の承認リクエストがある場合、[認証] ページにリクエストのステータスが表示されます。このページから、保留中のリクエストを承認することができます。

1. 承認するアグリゲータアカウントを選択し、[承認] を選択します。

   このアカウントから AWS Config データを収集するアクセス許可をアグリゲータアカウントに付与することを確認する確認メッセージが表示されます。

2. 再度 [承認] を選択し、アグリゲータアカウントへのアクセス権限の付与を確認します。

   認証のステータスが、[認証のリクエスト] から [承認済] に変わります。

アクセス権限の承認期間

ソースアカウントを個人アカウントアグリゲータに追加するには、アクセス権限の承認が必要です。承認待ちのリクエストは、個人アカウントアグリゲータによるソースアカウントの追加後 7 日間有効です。

Adding Authorization (AWS CLI)

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. 次のコマンドを入力します。

```
aws configservice put-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

3. 次のような出力が表示されます:

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

設定 AWS Config およびコンプライアンスデータを収集するためのアグリゲータアカウントの認可の削除

認可とは、 AWS Config 設定とコンプライアンスデータを収集するためにアグリゲータアカウントとリージョンに付与するアクセス許可を指します。 AWS Organizationsの一部であるソースアカウントを集約する場合、承認は必要ありません。 AWS Config コンソールまたは を使用して AWS CLI 、認可を削除できます。

トピック

- 考慮事項
- 認証の削除

考慮事項

アグリゲータには、個別アカウントアグリゲータと組織アグリゲータの 2 種類があります

個人アカウントアグリゲータの場合、外部アカウントとリージョン、組織のメンバーアカウントとリージョンの両方を含め、希望するすべてのソースアカウントとリージョンの承認が必要です。

組織アグリゲータの場合、認可は AWS Organizations サービスと統合されているため、組織メンバーアカウントリージョンに認可は必要ありません。

アグリゲータ AWS Config はユーザーに代わって を自動的に有効にしません

AWS Config ソースアカウントとリージョンで AWS Config データを生成するには、いずれかのタイプのアグリゲータのソースアカウントとリージョンで を有効にする必要があります。

認証の削除

Deleting Authorization (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. 認証を削除するアグリゲータアカウントを選択し、[削除] を選択します。

   警告メッセージが表示されます。この認可を削除すると、 AWS Config データはアグリゲータアカウントと共有されなくなります。

3. 再度 [削除] を選択して、選択を確定します。

   これで、アグリゲータのアカウントが削除されました。

Deleting Authorization (AWS CLI)

次のコマンドを入力します。

```
aws configservice delete-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

成功すると、コマンドは追加の出力なしで実行されます。

のアグリゲータの表示 AWS Config

AWS Config コンソールまたは を使用して、アグリゲータ AWS CLI を表示できます。

Viewing Aggregators (Console)

でコンフォーマンスパックを表示するには AWS Management Console、「アグリゲータダッシュボード」を参照してください。

Viewing Aggregators (AWS CLI)

1. 次のコマンドを入力します。

   ```
   aws configservice describe-configuration-aggregators
   ```

2. ソースアカウントに応じて、次のような出力が表示されます。

   個別のアカウントの場合

   ```
   {
       "ConfigurationAggregators": [
           {
               "ConfigurationAggregatorArn":
    "arn:aws:config:Region:AccountID:config-aggregator/config-aggregator-floqpus3",
               "CreationTime": 1517942461.442,
               "ConfigurationAggregatorName": "MyAggregator",
               "AccountAggregationSources": [
                   {
   ```

```
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

または

組織の場合

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

のマルチアカウントマルチリージョンデータ集約のトラブルシューティング AWS Config

AWS Config は、次のいずれかの理由でソースアカウントからデータを集約しない場合があります。

発生した問題	この操作を行います
AWS Config は、組織内のアカウントのソースアカウントで有効になっていません。	ソースアカウント AWS Config で を有効にし、アグリゲータアカウントにデータの収集を許可します。
アグリゲータアカウントに承認が与えられていない。	ソースアカウントにサインインし、アグリゲータアカウントに AWS Config データを収集する権限を付与します。
一時的な問題により、データの集約ができない可能性があります。	データの集約には遅延が発生する可能性があります。数分待ちます。

AWS Config は、次のいずれかの理由で組織からデータを集約しない場合があります。

発生した問題	この操作を行います
AWS Config IAM ロールが無効であるため、 は組織の詳細にアクセスできません。	IAM ロールを作成するか、IAM ロールのリストから有効な IAM ロールを選択します。 **Note** IAM ロールが 7 日以上無効な場合、 は組織全体のデータ AWS Config を削除します。
AWS Config サービスアクセスは組織内で無効になっています。	`EnableAWSServiceAccess` API AWS Organizations を使用して、 AWS Config と の統合を有効にできます。コンソールで組織を追加を選択すると、 は AWS Config と の統合 AWS Config を自動的に有効にします AWS Organizations。
AWS Config 組織ですべての機能が有効になっていないため、 は組織の詳細にアクセスできません。	AWS Organizations コンソールですべての機能を有効にします。

発生した問題	この操作を行います
アカウントの追加、アカウントの削除、サービスアクセスの有効化、サービスアクセスの無効化などの組織変更は、中東 (バーレーン) とアジアパシフィック (香港) のリージョンではすぐに更新されません。	組織変更には 2 時間の遅延が発生する可能性があります。2 時間待ってから、組織変更をすべて確認してください。

を使用したリソースの AWS 現在の設定状態のクエリ AWS Config

高度なクエリのプレビュー機能を導入すると、生成人工知能 (生成 AI) 機能を使用して平易な英語でプロンプトを入力し、すぐに使用できるクエリ形式に変換できます。詳細については、「Natural language query processor for advanced queries」を参照してください。

を使用して AWS Config 、1 つのアカウントとリージョン、または複数のアカウントとリージョンの設定プロパティに基づいて、 AWS リソースの現在の設定状態をクエリできます。が AWS Config サポートする AWS リソースのリスト全体で、現在のリソース状態メタデータに対してプロパティベースのクエリを実行できます。サポートされているリソースタイプのリストの詳細については、「Supported Resource Types for Advanced Queries」を参照してください。

高度なクエリ機能では、単一のクエリエンドポイントとクエリ言語を使用して、現在のリソース状態のメタデータを取得できます。サービス固有の記述用 API コールを実行する必要はありません。設定アグリゲータを使用して、複数のアカウントと AWS リージョンにわたって中央アカウントから同じクエリを実行できます。

トピック

- 機能
- のクエリコンポーネント AWS Config
- の SQL クエリエディタを使用したクエリ AWS Config （コンソール）
- の AWS Config SQL クエリエディタを使用したクエリ (AWS CLI）
- AWS Config 高度なクエリ用の自然言語クエリプロセッサ
- のクエリの例 AWS Config
- AWS Configの関係クエリの例
- 制限
- 高度なクエリの CIDR 表記/IP 範囲の動作
- 高度なクエリの配列動作内の複数のプロパティ
- リージョンのサポート

機能

AWS Config は、構造化クエリ言語 (SQL) SELECT構文のサブセットを使用して、現在の設定項目 (CI) データに対してプロパティベースのクエリと集計を実行します。このクエリは、タグやリソース識別子との一致から、バージョニングが無効になっているすべての Amazon S3 バケットの表示など、複雑性の高いクエリまで多岐にわたります。これにより、 AWS サービス固有の API コールを実行せずに、必要な現在のリソース状態を正確にクエリできます。

また、集計関数 (例: AVG、COUNT、MAX、MIN、SUM) をサポートしています。

以下の場合は、高度なクエリを使用することができます。

- インベントリ管理 (例: 特定のサイズの Amazon EC2 インスタンスのリストの取得)。
- セキュリティとオペレーションのインテリジェンス (例: 特定の設定プロパティーが有効または無効になっているリソースのリストの取得)。
- コスト最適化 (例: どの EC2 インスタンスにもアタッチされていない Amazon EBS ボリュームのリストの識別)。
- コンプライアンスデータ (例: すべてのコンフォーマンスパックとそのコンプライアンスステータスのリストの取得)。

AWS SQL クエリ言語の使用方法の詳細については、「SQL (構造化クエリ言語) とは」を参照してください。

のクエリコンポーネント AWS Config

AWS Config 詳細SELECTクエリの SQL クエリコンポーネントは次のとおりです。

概要

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

パラメータ

[WHERE condition]

指定した condition に従って結果をフィルタ処理します。

比較演算子

- = (等しい)
- IN (メンバーシップを一覧表示)
- BETWEEN (範囲チェック)

ロジック演算子

- AND
- OR
- NOT

[GROUP BY プロパティ]

指定されたプロパティの値が一致する行のグループに結果セットを集約します。

GROUP BY 句は集計に適用されます。

[ORDER BY property [ASC | DESC] [, property [ASC | DESC] ...]]

結果セットを 1 つ以上の出力 properties でソートします。

この句に複数のプロパティが含まれる場合、結果セットは、property に従ってソートされ、次の最初のプロパティの値と一致する値を持つ行に 2 番目の property が適用されます。以降同様の処理が行われます。

例

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

の SQL クエリエディタを使用したクエリ AWS Config（コンソール）

高度なクエリのプレビュー機能を導入すると、生成人工知能 (生成 AI) 機能を使用して平易な英語でプロンプトを入力し、すぐに使用できるクエリ形式に変換できます。詳細については、「Natural language query processor for advanced queries」を参照してください。

AWS サンプルクエリを使用するか、カスタムクエリとして という名前の独自のクエリを作成できます。

考慮事項

前提条件

次のいずれかの AWS マネージドポリシーを使用している場合は、クエリを実行して保存するために必要なアクセス許可が付与されます。AWSServiceRoleForConfig (サービスにリンクされたロール) または AWS_ConfigRole。

それ以外の場合は、AWSConfigUserAccess AWS 管理ポリシーに含まれるアクセス許可が必要です。

クエリできるプロパティのリスト

更新されたプロパティのリストとそのデータ型は、[GitHub] より入手できます。

高度なクエリとアグリゲータ

アグリゲーターでクエリを実行するには、アグリゲーターを作成します。詳細については、「のアグリゲータの作成 AWS Config」を参照してください。

アグリゲーターがすでに設定されている場合は、クエリのスコープでアグリゲーターを選択し、そのアグリゲーターで高度なクエリを実行します。アグリゲータを選択するときは、クエリステートメントに AWS アカウント ID と AWS リージョンを追加して、その情報を結果に表示することを検討してください。

AWS サンプルクエリを使用する

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。

2. 1 つのアカウントとリージョン、または複数のアカウントとリージョンのリソース設定をクエリするには、左側のナビゲーションから [Advanced queries (高度なクエリ)] を選択します。
3. [Advanced queries (高度なクエリ)] ページで、クエリのリストから適切なクエリを選択します。名前、説明、作成者、またはタグのいずれかで、クエリのリストをフィルタリングできます。AWS クエリをフィルタリングするには、[作成者]を選択して AWS と入力します。選択したクエリは、SQL クエリエディタに表示されます。選択したクエリはニーズに合わせて編集できます。
4. このクエリを新しいクエリに保存するには、[Save As (名前を付けて保存)] を選択します。
   - [Query Name (クエリ名)] フィールドで、クエリの名前を更新します。
   - [Description (説明)] フィールドで、クエリの説明を更新します。
   - このクエリには、最大 50 個の一意のタグを入力できます。
   - [Save (保存)] を選択します。
5. [Run (実行)] を選択します。クエリ結果は、クエリエディタの下の表に表示されます。
6. クエリ結果を CSV または JSON 形式でエクスポートするには、[Export as (エクスポート)] を選択します。

カスタムクエリの作成

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. 1 つのアカウントとリージョン、または複数のアカウントとリージョンのリソース設定をクエリするには、左側のナビゲーションから [Advanced queries (高度なクエリ)] を選択します。
3. カスタムクエリを作成するには、[New query (新しいクエリ)] を選択します。

   カスタムクエリを表示または編集するには、名前、説明、作成者、またはタグでクエリをフィルタリングします。カスタムクエリをフィルタリングするには、[Creator (作成者)] を選択し、[Custom (カスタム)] と入力します。
4. [Query editor (クエリエディタ)] ページで、このアカウントとリージョンに対して独自のクエリを作成します。また、適切なアグリゲーターを選択して、複数のアカウントとリージョンのクエリを作成することもできます。
5. このクエリに変更を加える場合は、編集してください。このクエリを保存するには、[Save Query (クエリの保存)] を選択します。
   - [Query Name (クエリ名)] フィールドで、クエリの名前を更新します。

- [Description (説明)] フィールドで、クエリの説明を更新します。
- このクエリには、最大 50 個の一意のタグを入力できます。
- [Save (保存)] を選択します。

6. [Run (実行)] を選択します。クエリ結果は、クエリエディタの下の表に表示されます。
7. クエリ結果を CSV または JSON 形式でエクスポートするには、[Export as (エクスポート)] を選択します。

の AWS Config SQL クエリエディタを使用したクエリ (AWS CLI)

AWS CLI は、 AWS のサービスを管理するための統合ツールです。ダウンロードと設定のツールを 1 つだけ使用すると、コマンドラインから複数の AWS サービスを制御したり、スクリプトを使用して自動化したりできます。の詳細 AWS CLI と AWS CLI ツールのインストール手順については、「AWS Command Line Interface ユーザーガイド」の以下を参照してください。

- AWS Command Line Interface ユーザーガイド
- AWS Command Line Interfaceのセットアップ

必要に応じて、 と入力`aws configure`して、高度なクエリが利用可能な AWS リージョンを使用する AWS CLI ように を設定します。

考慮事項

前提条件

次のいずれかの管理 AWS ポリシーを使用している場合は、クエリを実行して保存するために必要なアクセス許可が AWSServiceRoleForConfig (サービスにリンクされたロール) または AWS_ConfigRole に付与されます。

それ以外の場合は、AWSConfigUserAccess AWS 管理ポリシーに含まれるアクセス許可が必要です。

クエリできるプロパティのリスト

更新されたプロパティのリストとそのデータ型は、[GitHub] より入手できます。

高度なクエリとアグリゲータ

アグリゲーターでクエリを実行するには、アグリゲーターを作成します。詳細については、「のアグリゲータの作成 AWS Config」を参照してください。

アグリゲーターがすでに設定されている場合は、クエリのスコープでアグリゲーターを選択し、そのアグリゲーターで高度なクエリを実行します。アグリゲータを選択するときは、クエリステートメントに AWS アカウント ID と AWS リージョンを追加して、その情報を結果に表示することを検討してください。

リソース設定データのクエリ

クエリエディタ (AWS CLI) を使用して、単一のアカウントとリージョンのリソース設定データをクエリするには

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. リソース設定データをクエリするには、次のコマンドを入力します。

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

クエリに応じて、出力は次のようになります。

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

クエリエディタ (AWS CLI) を使用して、複数のアカウントとリージョンのリソース設定データをクエリするには

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. リソース設定データをクエリするには、次のコマンドを入力します。

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

クエリに応じて、出力は次のようになります。

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> 高度なクエリで `AWS::IAM::User`、`AWS::IAM::Group`、`AWS::IAM::Role`、および `AWS::IAM::Policy` リソースタイプを使用する場合は、`awsRegion = 'global'` を使用します。

クエリの保存

1. コマンドプロンプトまたはターミナルウィンドウを開きます。
2. 次のコマンドを入力してクエリを保存します。

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. クエリに応じて、出力は次のようになります。

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` は省略可能です。タグを渡すと、保存されたタグは `list-stored-queries` および `get-stored-query` のどちらからも返されません。`list-tag-for-resources` を使用して、保存されたクエリに関連するタグを取得する必要があります。
> `--description` は、クエリの作成時または更新時に使用するオプションです。

保存されたクエリをすべて表示

1. 保存されているすべてのクエリのリストを表示するには、次のコマンドを入力します。

```
aws configservice list-stored-queries
```

2. クエリに応じて、出力は次のようになります。

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
```

```
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
    ]
}
}
```

保存されたクエリの詳細の取得

1. 保存されたクエリの詳細を取得するには、次のコマンドを入力します。

```
aws configservice get-stored-query --query-name cli-test
```

2. クエリに応じて、出力は次のようになります。

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

保存されたクエリの削除

- 保存されたクエリを削除するには、次のコマンドを入力します。

```
aws configservice delete-stored-query --query-name cli-test
```

成功すると、コマンドは追加の出力なしで実行されます。

AWS Config 高度なクエリ用の自然言語クエリプロセッサ

> 高度なクエリの自然言語クエリプロセッサは、 のプレビューリリースであり AWS Config 、変更される可能性があります。

高度なクエリ用の自然言語クエリプロセッサは、生成人工知能 (生成 AI) テクノロジーである Amazon Bedrock を使用しています。これにより、平易な英語でプロンプトを入力し、すぐに使用できるクエリ形式に変換できます。自然言語クエリプロセッサを使用すると、 AWS アカウント または AWS 組織全体でクエリを実行できます。

プロンプトは質問またはステートメントのいずれかにできます。例えば、「2024 年 1 月 1 日以降に作成されるロードバランサーはどれか?」や 「ノード js 16 を実行しているすべての lambda 関数を一覧表示してください」などのプロンプトを入力できます。

考慮事項

自然言語クエリプロセッサは、次のアクションを実行できません。

- 英語以外の言語からクエリを生成します。
- 高度なクエリに関連しないプロンプトからクエリを生成します。
- 1000 文字を超えるプロンプトからクエリを生成します。
- フォローアップの修正または以前のセッションからクエリを生成します。
- 生成されたコードについて説明します。

自然言語クエリプロセッサを使用したクエリ

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. 1 つのアカウントとリージョン、または複数のアカウントとリージョンのリソース設定をクエリするには、左側のナビゲーションから [Advanced queries (高度なクエリ)] を選択します。
3. [高度なクエリ] ページで [新しいクエリ] を選択し、 クエリエディタに移動します。
   - (オプション) アグリゲーターでクエリを実行するには、アグリゲーターを作成します。詳細については、「のアグリゲータの作成 AWS Config」を参照してください。

- 既にアグリゲータが設定されている場合は、クエリのスコープでアグリゲーターを選択し、そのアグリゲーターで高度なクエリを実行します。アグリゲータを選択するときは、クエリステートメントに AWS アカウント ID と AWS リージョンを追加して、その情報を結果に表示することを検討してください。

4. クエリエディタで、「自然言語クエリプロセッサ」セクションに移動します。プロンプトを平易な英語で入力し、[生成] を選択します。例については、「プロンプトの例」を参照してください。
5. クエリを生成した後、[コピー] (Ctrl+C と機能的に同じ) を選択してクエリをクリップボードにコピーするか、[エディタに移動] を選択します。エディタに入力されたら、生成されたクエリをニーズに合わせて編集できます。
6. このクエリを新しいクエリに保存するには、[Save As (名前を付けて保存)] を選択します。
   - [Query Name (クエリ名)] フィールドで、クエリの名前を更新します。
   - [Description (説明)] フィールドで、クエリの説明を更新します。
   - このクエリには、最大 50 個の一意のタグを入力できます。
   - [Save (保存)] を選択します。
7. [Run (実行)] を選択します。クエリ結果は、クエリエディタの下の表に表示されます。
8. クエリ結果を CSV または JSON 形式でエクスポートするには、[Export as (エクスポート)] を選択します。

> **Note**
> クエリの結果はページ分割されます。エクスポートすると、最大 500 の結果がエクスポートされます。
> また、API を使用してすべての結果を取得することもできます。結果はページ分割され、一度に 100 件の結果を取得できます。

プロンプトの例

以下は、例として使用できるプロンプトと生成クエリです。

Example: 2024 年 1 月 1 日より後に作成されるロードバランサーはどれですか？

プロンプト: What load balancers were created after January 1, 2024?

生成されたクエリ:

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: パブリックにアクセス可能なすべての RDS データベースインスタンスはどれですか？

プロンプト: Which of my RDS database instances are publicly accessible?

生成されたクエリ:

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: 過去 1 年間に作成された EC2 インスタンスの数は?

プロンプト: How many EC2 instances were created in last one year?

生成されたクエリ:

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
```

```
AND
    '2024-05-10T16:56:25.000Z'
```

Example: 各 AWS アカウントはにいくつの EC2 インスタンスがありますか？

プロンプト: How many EC2 instances do I have in each of my AWS アカウント?

生成されたクエリ:

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: マネージドポリシー AdministratorAccess がアタッチされている IAM ロールはどれですか？

プロンプト: Which IAM roles have the managed policy AdministratorAccess attached?

生成されたクエリ:

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: 暗号化なしの EBS ボリューム

プロンプト: EBS volumes without encryption

生成されたクエリ:

```
SELECT
    accountId
```

```
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: 非準拠リソースを取得する

プロンプト: Get noncompliant resources

生成されたクエリ:

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: ノード js 16 を実行しているすべての lambda 関数を一覧表示する

プロンプト: List all my lambda function that is running node js 16

生成されたクエリ:

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: 今後 30 日間で期限切れになる ACM 証明書はどれですか？

プロンプト: What ACM certificates expire the next 30 days?

生成されたクエリ:

```
SELECT
    resourceId,
```

```
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> 生成されたクエリの時間は、プロンプトを入力する時間によって異なります。

フィードバックの提供

自然言語クエリプロセッサに関する全体的なフィードバックや、特定の生成されたクエリに関するフィードバックを提供できます。

自然言語クエリプロセッサに関するフィードバックの提供

自然言語クエリプロセッサの右上に表示される [フィードバックを提供] ボタンを選択します。満足度または不満を入力し、自然言語クエリをより役立つものに AWS Config する方法に関するフィードバックを提供できます。

> **Note**
>
> 個人情報、商業的機密情報、または機密情報を開示しないでください。

特定の生成されたクエリに関するフィードバックの提供

生成されたクエリの下に表示される高評価または低評価ボタンを選択して、生成されたクエリに関するフィードバックを提供することができます。

リージョンのサポート

自然言語クエリプロセッサは、次のリージョンでサポートされています。

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

のクエリの例 AWS Config

次のクエリ例を表示します。

Query to list all EC2 instances with AMI ID ami-12345

クエリ:

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

結果:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
```

```
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their AWS Config rules compliance status

クエリ:

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

結果:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

クエリ:

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

結果:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

クエリ:

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

結果:

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
```

```
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

クエリ:

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

結果:

```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
```

```
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
```

```
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

AWS Configの関係クエリの例

次の関係クエリの例を表示します。

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

または

```
SELECT
    resourceId
```

```
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

制限

> **Note**
>
> アドバンストクエリは、設定レコーダーによって記録されるように設定されていないリソースのクエリをサポートしていません。リソースが検出されたが、設定レコーダーによって記録されるように設定されていない場合configurationItemStatus、ResourceNotRecordedで を使用して設定項目 (CIs) AWS Config を作成します。アグリゲーターはこれらの CI を集約しますが、高度なクエリでは ResourceNotRecorded での CI のクエリをサポートしていません。レコーダー設定を更新して、クエリするリソースタイプを記録できるようにしてください。

SQL SELECT のサブセットとして、クエリ構文には次の制限があります。

- ALL、AS、DISTINCT、FROM、HAVING、JOIN、および UNION などのクエリのキーワードはサポートされていません。NULL 値のクエリはサポートされていません。
- クエリで優先度フィールドを直接作成するための複雑なCASEステートメントはサポートされていません。
- サードパーティーリソースに対するクエリはサポートされていません。高度なクエリを使用して取得したサードパーティーリソースでは、設定フィールドが NULL に設定されます。
- SQL クエリで展開されるネスト構造 (タグなど) はサポートされていません。
- 削除されたリソースのクエリはサポートされていません。削除されたリソースを検出するには、「によって検出されたリソースの検索 AWS Config」を参照してください。
- すべての SELECT 列の省略表現 (つまり SELECT *) では、CI の最上位のスカラープロパティのみ選択されます。スカラープロパティは、accountId、awsRegion、arn、availabilityZone、configurationItemCaptureTime、re が返ります。
- ワイルドカードの制限:
  - ワイルドカードは、プロパティ値でのみサポートされており、プロパティキーではサポートされていません (例: ...WHERE someKey LIKE 'someValue%' はサポートされますが、...WHERE 'someKey%' LIKE 'someValue%' はサポートされません)。
  - サフィックスのワイルドカードのみをサポートします (例: ...LIKE 'AWS::EC2::%' と ...LIKE 'AWS::EC2::_' はサポートされますが、...LIKE '%::EC2::Instance' と ...LIKE '_::EC2::Instance' はサポートされません)。

- ワイルドカードの一致は、3 文字以上でなければなりません (例: `...LIKE 'ab%'` と `...LIKE 'ab_'` は許可されていませんが、`...LIKE 'abc%'` と `...LIKE 'abc_'` は許可されています)。

> **Note**
>
> 「_」(単一のアンダースコア) もワイルドカードとして扱われます。

- 集約の制限:
  - 集計関数は、単一の引数またはプロパティのみ受け入れることができます。
  - 集計関数では、その他の関数を引数として取ることはできません。
  - `GROUP BY` は集約関数を参照する `ORDER BY` 句と組み合わせて、単一プロパティのみ含めることができます。
  - その他のすべての集約 `GROUP BY` 句には 3 つまでのプロパティを含めることができます。
  - ページ割りは、`ORDER BY` 句に集計関数がある場合を除き、すべての集約クエリでサポートされています。例えば、Y が集計関数の場合、`GROUP BY X, ORDER BY Y` は機能しません。
  - 集約では、`HAVING` 句はサポートされていません。
- 不一致の識別子に関する制限事項:

  不一致の識別子とは、スペルは同じで、アルファベットの大文字と小文字が異なるプロパティのことです。詳細クエリは、不一致の識別子を含むクエリの処理をサポートしていません。例:
  - スペルがまったく同じで、アルファベットの大文字と小文字が異なる 2 つのプロパティ (`configuration.dbclusterIdentifier` および `configuration.dBClusterIdentifier`)。
  - 一方のプロパティがもう一方のプロパティのサブセットで、アルファベットの大文字と小文字が異なる 2 つのプロパティ (`configuration.ipAddress` および `configuration.ipaddressPermissions`)。

高度なクエリの CIDR 表記/IP 範囲の動作

CIDR 表記は、検索用の IP 範囲に変換されます。

これは、"=" と "BETWEEN" が厳密な IP 範囲ではなく、提供された IP が含まれるすべての範囲を検索することを意味します。

厳密な IP 範囲を検索するには、範囲外の IP を除外するための条件を追加する必要があります。

Example 正確な CIDR ブロック 10.0.0.0/24 の検索

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Example 正確な IP アドレス 192.168.0.2/32 の検索

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

高度なクエリの配列動作内の複数のプロパティ

オブジェクトの配列内の複数のプロパティに対してクエリを実行する場合、一致はすべての配列要素に対して計算されます。

例えば、ルール A と B を持つリソース R の場合、リソースはルール A に準拠していますが、ルール B には準拠していません。リソース R は次のように保存されます。

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

R は、このクエリによって返されます。

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
```

```
AND configuration.configRuleList.configRuleName = 'A'
```

最初の条件`configuration.configRuleList.complianceType = 'non_compliant'`は R.configRuleList のすべての要素に適用されます。R には complianceType = 'non_compliant' のルール (ルール B) があるため、条件は true と評価されます。

2 番目の条件`configuration.configRuleList.configRuleName`は R.configRuleList のすべての要素に適用されます。R には configRuleName = 'A' のルール (ルール A) があるため、条件は true として評価されます。両方の条件が true であるため、R が返されます。

リージョンのサポート

高度なクエリは、次のリージョンでサポートされています。

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (オハイオ)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
米国東部 (バージニア北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
米国西部 (北カリフォルニア)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
米国西部 (オレゴン)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
アフリカ (ケープタウン)	af-south-1	config.af-south-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (香港)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
アジアパシフィック (ハイデラバード)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
アジアパシフィック (ジャカルタ)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
アジアパシフィック (マレーシア)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
アジアパシフィック (メルボルン)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
アジアパシフィック (大阪)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
アジアパシフィック (ソウル)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
アジアパシフィック (シドニー)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
アジアパシフィック (台北)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
アジアパシフィック (タイ)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
カナダ西部 (カルガリー)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
欧州 (フランクフルト)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧州 (アイルランド)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
ヨーロッパ (ミラノ)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧州 (スペイン)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧州 (ストックホルム)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧州 (チューリッヒ)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
イスラエル (テルアビブ)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
メキシコ (中部)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
中東 (バーレーン)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中東 (アラブ首長国連邦)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config データの削除

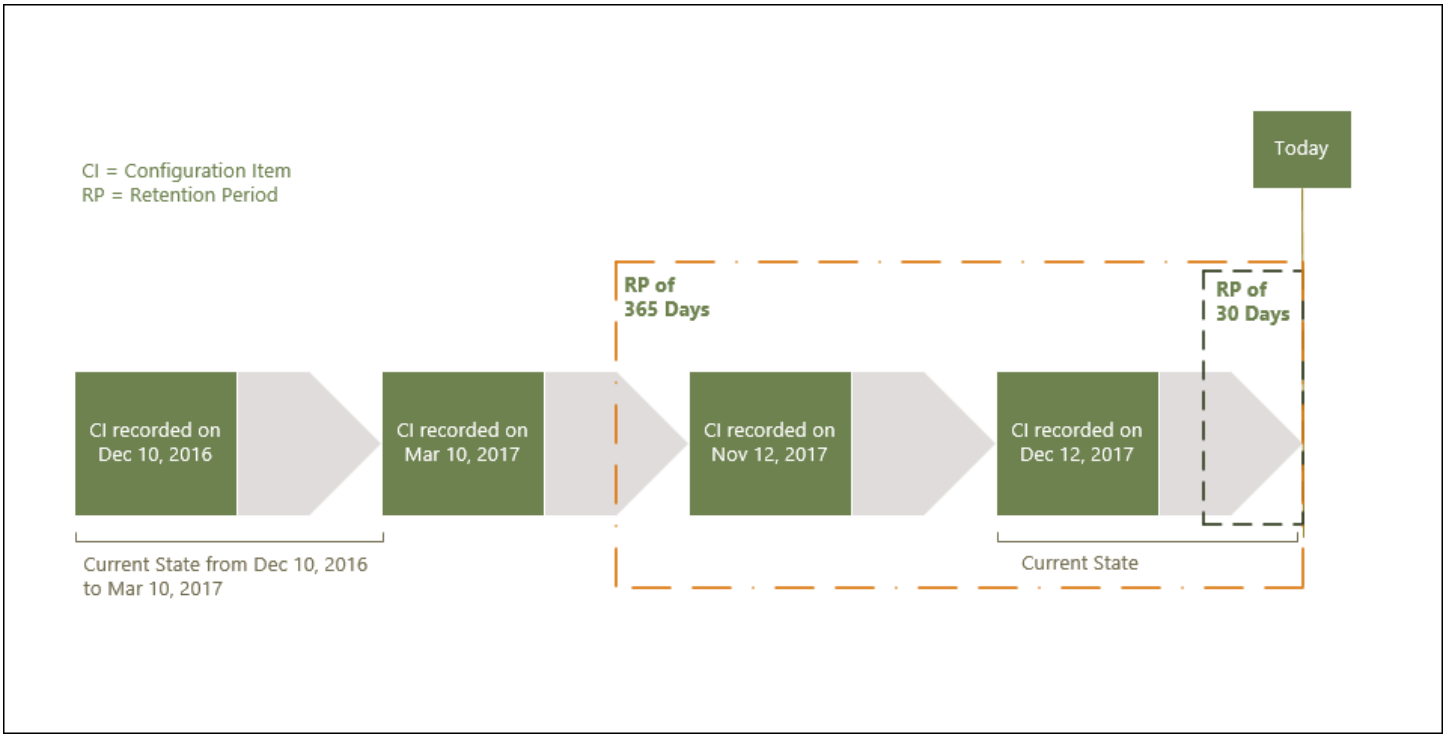
> **Note**
>
> は、設定スナップショットと設定履歴ファイルの送信に Amazon Simple Storage Service (Amazon S3) と Amazon Simple Notification Service (Amazon SNS) AWS Config を使用しますが、 には独自のデータストアと保持ポリシー AWS Config があります。このページの情報は に固有です AWS Config。Amazon S3 と Amazon SNS には、それぞれ独自のデータストアポリシーとリテンションポリシーがあります。

AWS Config では、 の保持期間を指定してデータを削除できます`ConfigurationItems`。保持期間を指定すると、 はその指定された期間 `ConfigurationItems` AWS Config を保持します。最小 30 日から最大 7 年 (2557 日) の期間を選択できます。 は、指定した保持期間より古いデータ AWS Config を削除します。保持期間を指定しない場合、 AWS Config では、デフォルト期間である 7 年間 (2557 日間)、`ConfigurationItems` を保存します。記録がオンになっている場合、リソースの現在の状態は、`ConfigurationItem` の記録時と、次の変更 (新しい `ConfigurationItem`) が記録されるまでです。

保持期間の動作を把握するために、タイムラインを確認しましょう。

- 記録がオンになっている場合、リソースの現在の状態は常に存在し、`ConfigurationItem` が記録される日付に関係なく削除することはできません。
- が新しい AWS Config を記録すると`ConfigurationItems`、指定した保持期間に応じて前の `ConfigurationItems`が削除されます。

次のタイムライン AWS Config では、 は次の日付`ConfigurationItems`を記録します。タイムラインの目的上、今日は 2018 年 5 月 24 日として表示されます。



次の表では、選択した保持期間に基づき、 AWS Config タイムラインに表示する `ConfigurationItems` を示します。

保持期間	タイムラインに表示される設定項目	説明
30 日間	2017 年 12 月 12 日	`ConfigurationItem` が記録され、本日 (2018 年 5 月 24 日) まで有効な場合に、2017 年 12 月 12 日から開始したリソースの現在の状態。記録がオンになっている場合、現在の状態は常に存在します。
365 日間	2017 年 12 月 12 日、2017 年 11 月 12 日、2017 年 3 月 10 日	この保持期間では、現在の状態 2017 年 12 月 12 日、および以前の `ConfigurationItems` である 2017 年 11 月 12 日と 2017 年 3 月 10 日を示します。 設定状態は、365 日前の現在の状態を表していたため、2017 年 3 月 10

保持期間	タイムラインに表示される設定項目	説明
		日の `ConfigurationItem` がタイムラインに表示されます。

保持期間を指定すると、 AWS Config APIs指定された保持期間より古い状態`ConfigurationItems`を表す を返さなくなります。

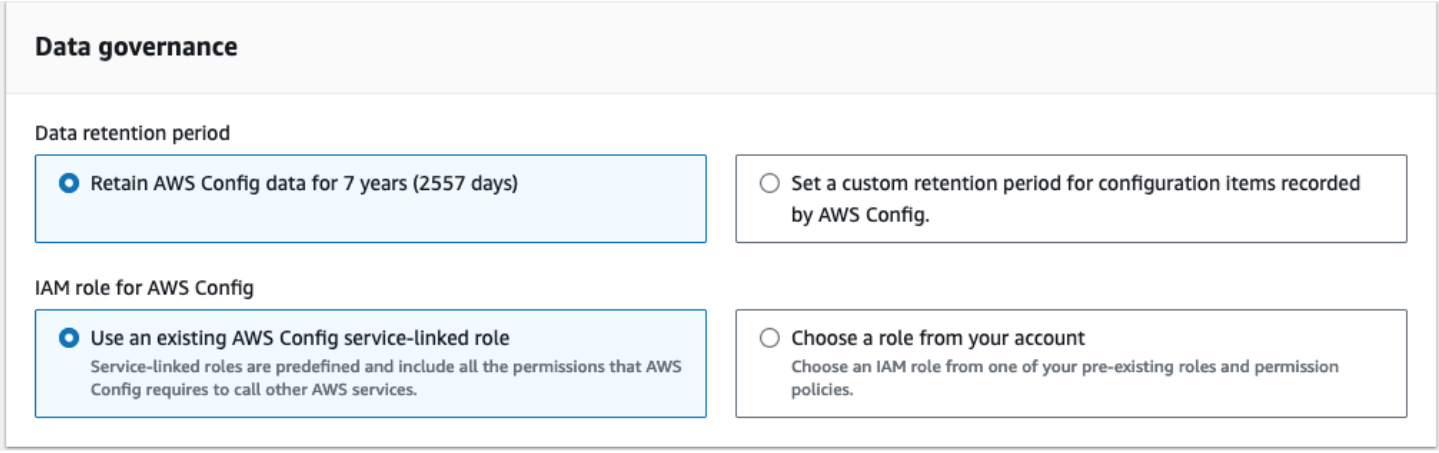
> **Note**
>
> - AWS Config 録画がオフになっている`ConfigurationItems`場合、 は を記録できません。
> - AWS Config IAM ロールのアクセス許可が不十分な`ConfigurationItems`場合、 は を記録できません。詳細については、「割り当てられた IAM ロールのアクセス許可 AWS Config」を参照してください。

でのデータ保持期間の設定 AWS Management Console

では AWS Management Console、データ保持期間を選択しない場合、デフォルトの期間は 7 年または 2557 日です。

設定項目に対して、カスタムのデータ保持期間を設定するには、[Checkbox (チェックボックス)] をオンにします。1 年、3 年、5 年、またはカスタムの期間を選択できます。カスタムの期間を設定する場合は、30 日 ~ 2557 日の範囲の数値を入力します。

次の画像は、[データガバナンス] でデータ保持期間を設定できる場所を示しています。 AWS Config コンソールから設定の編集ページでデータガバナンスにアクセスするには、左側のナビゲーションバーで設定を選択し、編集を選択します。


Data governance
Data retention period
Retain AWS Config data for 7 years (2557 days)
Set a custom retention period for configuration items recorded by AWS Config.
IAM role for AWS Config
Use an existing AWS Config service-linked role
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.
Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.

のセキュリティ AWS Config

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — クラウドで AWS AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。が適用されるコンプライアンスプログラムの詳細については AWS Config、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS Config。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成する AWS Config ように を設定する方法を示します。

トピック

- でのデータ保護 AWS Config
- の Identity and Access Management AWS Config
- でのインシデント対応 AWS Config
- のコンプライアンス検証 AWS Config
- の耐障害性 AWS Config
- のインフラストラクチャセキュリティ AWS Config
- サービス間の混乱した代理の防止
- のセキュリティのベストプラクティス AWS Config

でのデータ保護 AWS Config

責任 AWS 共有モデル、Config AWS でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK AWS を使用して Config AWS CLIまたは他の AWS のサービス を使用する場合も同様です。AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

保管時のデータの暗号化

データは、透過的なサーバー側の暗号化を使用して保存時に暗号化されます。これは、機密データの保護における負担と複雑な作業を減らすのに役立ちます。保管時に暗号化することで、セキュリティを重視したアプリケーションを構築して、暗号化のコンプライアンスと規制の要件を満たすことができます。

転送時のデータの暗号化

によって収集およびアクセスされるデータは AWS Config 、Transport Layer Security (TLS) で保護されたチャネルでのみ使用されます。

の Identity and Access Management AWS Config

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Config リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- が IAM と AWS Config 連携する方法
- のアイデンティティベースのポリシーの例 AWS Config
- AWS の 管理ポリシー AWS Config
- に割り当てられた IAM ロールのアクセス許可 AWS Config
- カスタマーマネージド設定レコーダーの IAM ロールの更新
- AWS Config 配信チャネルの Amazon S3 バケットのアクセス許可
- AWS Config 配信チャネルの KMS キーのアクセス許可
- Amazon SNS トピックへのアクセス許可
- AWS Config ID とアクセスのトラブルシューティング
- のサービスにリンクされたロールの使用 AWS Config

対象者

AWS Identity and Access Management (IAM) の使用方法は、作業内容によって異なります AWS Config。

サービスユーザー – AWS Config サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が提供されます。さらに多くの AWS Config 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者から適切な権限をリクエストするのに役に立ちます。 AWS Config機能にアクセスできない場合は、「AWS Config ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内の AWS Config リソースを担当している場合は、通常、 へのフルアクセスがあります AWS Config。サービスユーザーがどの AWS Config 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で IAM を使用する方法の詳細については AWS Config、「」を参照してくださいが IAM と AWS Config 連携する方法。

IAM 管理者 - 管理者は、 AWS Configへのアクセスを管理するポリシーの書き込み方法の詳細について確認する場合があります。IAM で使用できる AWS Config アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS Config。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーション ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して にアクセスすると、間接的 AWS にロールを引き受けることになります。

ユーザーの種類に応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 へのサインイン AWS アカウント方法」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、、AWS Directory Serviceアイデンティティセンターディレクトリ、または ID ソースを介して提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、独自の ID ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity

Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エ

ンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

が IAM と AWS Config 連携する方法

IAM を使用して へのアクセスを管理する前に AWS Config、使用できる IAM 機能を確認してください AWS Config。

で使用できる IAM 機能 AWS Config

IAM の機能	AWS Config サポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	いいえ
ポリシーアクション	はい
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	いいえ
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	はい
サービスリンクロール	はい

AWS Config およびその他の AWS のサービスがほとんどの IAM 機能とどのように連携するかの概要については、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

のアイデンティティベースのポリシー AWS Config

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、

ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

のアイデンティティベースのポリシーの例 AWS Config

AWS Config アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS Config。

内のリソースベースのポリシー AWS Config

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

のポリシーアクション AWS Config

ポリシーアクションのサポート:あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

AWS Config アクションのリストを確認するには、「サービス認可リファレンス」の「 で定義されるアクション AWS Config」を参照してください。

のポリシーアクションは、アクションの前に次のプレフィックス AWS Config を使用します。

```
config
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、`Describe` という単語で始まるすべてのアクションを指定するには次のアクションを含めます。

```
"Action": "config:Describe*"
```

AWS Config アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS Config。

のポリシーリソース AWS Config

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントには`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

AWS Config リソースタイプとその ARNs「 で定義されるリソース AWS Config」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、「AWS Configで定義されるアクション」を参照してください。

AWS Config アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS Config。

のポリシー条件キー AWS Config

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Condition` 要素 (または `Condition` ブロック) を使用すると、ステートメントが有効な条件を指定できます。`Condition` 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の `Condition` 要素を指定する場合、または 1 つの `Condition` 要素に複数のキーを指定する場合、 AWS では `AND` 論理演算子を使用してそれらを評価します。1 つの条

件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

AWS Config 条件キーのリストを確認するには、「サービス認可リファレンス」の「 の条件キー AWS Config」を参照してください。条件キーを使用できるアクションとリソースについては、「 で定義されるアクション AWS Config」を参照してください。

AWS Config アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS Config。

ACLs AWS Config

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

を使用した ABAC AWS Config

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

AWS Config リソースのタグ付けの詳細については、「」を参照してくださいAWS Config リソースのタグ付け。

での一時的な認証情報の使用 AWS Config

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報と AWS のサービス 連携する などの詳細については、AWS のサービス IAM ユーザーガイドの「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の方法 AWS Management Console を使用して にサインインする場合、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

の転送アクセスセッション AWS Config

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり

取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FASリクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS Configのサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。

> **Warning**
> サービスロールの権限を変更すると、 AWS Config の機能が破損する可能性があります。AWS Config が指示する場合にのみ、サービスロールを編集します。

のサービスにリンクされたロール AWS Config

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

AWS Config サービスにリンクされたロールの作成または管理の詳細については、「」を参照してください[のサービスにリンクされたロールの使用 AWS Config](#)。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

のアイデンティティベースのポリシーの例 AWS Config

デフォルトでは、 ユーザーおよびロールには、 AWS Config リソースを作成または変更する権限はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なア

クションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARN の形式など AWS Config、 で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」の「 のアクション、リソース、および条件キー AWS Config」を参照してください。 ARNs

トピック

- ポリシーに関するベストプラクティス
- にサインアップする AWS アカウント
- 管理アクセスを持つユーザーを作成する
- AWS Config コンソールを使用する
- 自分の権限の表示をユーザーに許可する
- への読み取り専用アクセス AWS Config
- へのフルアクセス AWS Config
- AWS Config ルール API アクションでサポートされているリソースレベルのアクセス許可
- マルチアカウント、マルチリージョンのデータ集約でサポートされるリソースレベルのアクセス許可。

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内の AWS Config リソースを誰かが作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。

- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 を保護し AWS IAM Identity Center、 を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの AWS アカウント 「ルートユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 AWS IAM Identity Center ユーザーガイド」の「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン「 ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」を参照してください。

AWS Config コンソールを使用する

AWS Config コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の AWS Config リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き AWS Config コンソールを使用できるようにするには、エンティティに AWS Config *AWSConfigUserAccess* AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

操作するアクセス許可をユーザーに付与する必要があります AWS Config。へのフルアクセスを必要とするユーザーの場合は AWS Config、 管理ポリシーへのフルアクセス AWS Configを使用します。

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- 以下のユーザーとグループ AWS IAM Identity Center：

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。
- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。
- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については、「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

```
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

への読み取り専用アクセス AWS Config

次の例は、 への読み取り専用アクセス`AWSConfigUserAccess`を許可する AWS マネージドポリシーを示しています AWS Config。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
```

```
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

このポリシーステートメントの `Effect` 要素で、アクションが許可されるか拒否されるかを指定します。`Action` 要素には、ユーザーによる実行を許可する特定のアクションを指定します。`Resource` 要素には、ユーザーがこれらのアクションを実行できる AWS リソースが一覧表示されます。 AWS Config アクションへのアクセスを制御するポリシーの場合、 `Resource`要素は常にに設定されます。`*`これは「すべてのリソース」を意味するワイルドカードです。

`Action` 要素の値は、サービスがサポートする API に対応しています。アクションの先頭に が付き`config:`、 AWS Config アクションを参照していることを示します。次の例に示すように、`*` ワイルドカード文字を `Action` 要素で使用できます。

- `"Action": ["config:*ConfigurationRecorder"]`

  これにより、ConfigurationRecorder」 (`StartConfigurationRecorder`、) で終わるすべての AWS Config アクションが許可されますStopConfigurationRecorder。

- `"Action": ["config:*"]`

  これにより、すべての AWS Config アクションが許可されますが、他の AWS サービスのアクションは許可されません。

- `"Action": ["*"]`

  これにより、すべての AWS アクションが許可されます。このアクセス許可は、アカウントの AWS 管理者として機能するユーザーに適しています。

読み取り専用ポリシーでは、`StartConfigurationRecorder`、`StopConfigurationRecorder`、`DeleteConfigurationRec`などのアクションに対するアクセス許可をユーザーに付与することはできません。このポリシーを持

つユーザーが、設定レコーダーの開始、停止、または削除を行うことはできません。 AWS Config アクションのリストについては、 AWS Config API リファレンスを参照してください。

へのフルアクセス AWS Config

次の例は、 へのフルアクセスを許可するポリシーを示しています AWS Config。これにより、すべての AWS Config アクションを実行するアクセス許可がユーザーに付与されます。また、Amazon S3 バケットのファイルの管理や、ユーザーが関連付けられているアカウントの Amazon SNS トピックの管理も行うことができます。

> **Important**
>
> このポリシーによって、広範なアクセスが許可されます。フルアクセスを付与する前にまず最小限のアクセス許可から開始し、必要に応じて追加のアクセス許可を付与することを検討してください。この方法は、寛容なアクセス許可から開始して、後でそれを厳しくするよりも安全です。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
```

```
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

AWS Config ルール API アクションでサポートされているリソースレベルのアクセス許可

リソースレベルのアクセス許可とは、ユーザーがアクションを実行できるリソースを指定する機能を指します。 は、特定の AWS Config ルール API アクションのリソースレベルのアクセス許可 AWS Config をサポートします。つまり、特定の AWS Config ルールアクションでは、ユーザーがそれら

のアクションを使用できる条件を制御できます。これらの条件には、アクションの要件や、ユーザーが使用できる特定のリソースなどがあります。

次の表は、現在リソースレベルのアクセス許可をサポートしている AWS Config ルール API アクションを示しています。各アクションでサポートされるリソースとその ARN についても説明しています。ARN の指定時、正確なリソース ID を指定できない (したくない) 場合などに、パスに * ワイルドカードを使用できます。

> **Important**
>
> AWS Config ルール API アクションがこのテーブルにリストされていない場合、リソースレベルのアクセス許可はサポートされていません。 AWS Config ルールアクションがリソースレベルのアクセス許可をサポートしていない場合は、アクションを使用するアクセス許可をユーザーに付与できますが、ポリシーステートメントのリソース要素に * を指定する必要があります。

API アクション	リソース
DeleteConfigRule	Config ルール arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DeleteEvaluationResults	Config ルール arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeComplianceByConfigRule	Config ルール arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeConfigRuleEvaluationStatus	Config ルール arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
GetComplianceDetailsByConfigRule	Config ルール arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutConfigRule	Config ルール

API アクション	リソース
	arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
StartConfigRulesEvaluation	Config ルール arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutRemediationConfigurations	修復の設定 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationConfigurations	修復の設定 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediationConfiguration	修復の設定 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
PutRemediationExceptions	修復の設定 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationExceptions	修復の設定 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

API アクション	リソース
DeleteRemediationExceptions	修復の設定 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

例えば、特定のルールで特定のユーザーに読み取りアクセスを許可して、書き込みアクセスを拒否するとします。

最初のポリシーでは、指定した AWS Config ルール`DescribeConfigRuleEvaluationStatus`でなどの読み取りアクションをルールに許可します。

JSON

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

2 番目のポリシーでは、特定の AWS Config ルールに対するルール書き込みアクションを拒否します。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-
rule-ID"
           }
      ]
   }
```

リソースレベルのアクセス許可を使用すると、読み取りアクセスを許可し、書き込みアクセスを拒否して、 AWS Config ルール API アクションに対して特定のアクションを実行できます。

マルチアカウント、マルチリージョンのデータ集約でサポートされるリソースレベルのアクセス許可。

ユーザーがマルチアカウントマルチリージョンのデータ集約に対して特定のアクションを実行する機能を管理するには、リソースレベルのアクセス許可を使用します。次の AWS Config `Aggregator` APIs、リソースレベルのアクセス許可をサポートしています。

- BatchGetAggregateResourceConfig
- DeleteConfigurationAggregator
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStatus
- GetAggregateComplianceDetailsByConfigRule
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary

- GetAggregateDiscoveredResourceCounts
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAggregator
- SelectAggregateResourceConfig

例えば、2 つのアグリゲーター `AccessibleAggregator` および `InAccessibleAggregator` を作成し、`AccessibleAggregator` へのアクセスを許可するが、`InAccessibleAggregator` へのアクセスは拒否する IAM ポリシーをアタッチすることで、特定のユーザーからのリソースデータへのアクセスを制限できます。

AccessibleAggregator の IAM ポリシー

このポリシーでは、指定した AWS Config Amazon リソースネーム (ARN) に対してサポートされているアグリゲーターアクションへのアクセスを許可します。この例では、 AWS Config ARN は ですarn:aws:config:ap-northeast-1:*AccountID*:config-aggregator/config-aggregator-mocpsqhs。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
```

```
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-mocpsqhs"
        }
    ]
}
```

InAccessibleAggregator の IAM ポリシー

このポリシーでは、指定した AWS Config ARN に対してサポートされているアグリゲーターアクションへのアクセスを拒否します。この例では、 AWS Config ARN は ですarn:aws:config:ap-northeast-1:*AccountID*:config-aggregator/config-aggregator-pokxzldx。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
```

```
}
```

デベロッパーグループのユーザーが、指定した AWS Config ARN でこれらのいずれかのアクションの実行を試みた場合、そのユーザーはアクセス拒否の例外を受け取ります。

ユーザーのアクセス許可の確認

作成したアグリゲーターを表示するには、次の AWS CLI コマンドを実行します。

```
aws configservice describe-configuration-aggregators
```

コマンドが正常に完了すると、アカウントに関連付けられているすべてのアグリゲーターの詳細を確認できます。この例では、`AccessibleAggregator` および `InAccessibleAggregator` のようになります。

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
```

```
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> `account-aggregation-sources` に、データを集約する AWS アカウント ID のカンマ区切りリストを入力します。アカウント ID を角括弧で囲み、必ず疑問符をエスケープします (例: `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"], \"AllAwsRegions\": true}]"`)。

`InAccessibleAggregator` へのアクセス、またはアクセス先となるアグリゲータを拒否するには、次の IAM ポリシーをアタッチします。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
```

```
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
}
```

次に、特定のアグリゲータのルールへのアクセスを制限する IAM ポリシーが動作していることを確認できます。

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

このコマンドではアクセス拒否の例外が返されます。

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

AWS の 管理ポリシー AWS Config

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、多くの一般的なユースケースにアクセス許可を付与するように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパ

ル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

詳細については「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS マネージドポリシー: AWSConfigServiceRolePolicy

AWS Config は、 という名前のサービスにリンクされたロールAWSServiceRoleForConfigを使用して、ユーザーに代わって他の AWS サービスを呼び出します。を使用して AWS Management Console を設定すると AWS Config、独自の AWS Identity and Access Management (IAM) サービスロールの代わりに SLR を使用するオプション AWS Config を選択すると、この AWS Config SLR がによって自動的に作成されます。

AWSServiceRoleForConfig SLR は管理ポリシー `AWSConfigServiceRolePolicy` を含んでいます。この管理ポリシーには、 AWS Config リソースの読み取り専用および書き込み専用アクセス許可と、 が AWS Config サポートする他の サービスのリソースの読み取り専用アクセス許可が含まれています。詳細については、「でサポートされているリソースタイプ AWS Config」および「のサービスにリンクされたロールの使用 AWS Config」を参照してください。

ポリシー:「AWSConfigServiceRolePolicy」ご覧ください。

> **推奨: サービスにリンクされたロールを使用する**
>
> 特定のユースケースがない限り、サービスにリンクされたロールを使用することをお勧めします。サービスにリンクされたロールは、 AWS Config が予想どおりに実行するのに必要なすべてのアクセス許可を追加します。サービスにリンクされた設定レコーダーなどの一部の機能では、サービスにリンクされたロールを使用する必要があります。

AWS 管理ポリシー: AWS_ConfigRole

AWS リソース設定を記録するには、リソースの設定の詳細を取得するための IAM アクセス許可 AWS Config が必要です。 AWS Configの IAM ロールを作成する場合は、管理ポリシー `AWS_ConfigRole` を使用してそれを IAM ロールに適用します。

この IAM ポリシーは、 が AWS リソースタイプのサポート AWS Config を追加するたびに更新されます。つまり AWS Config 、AWS_ConfigRole ロールにこの管理ポリシーがアタッチされている限り、 には、サポートされているリソースタイプの設定データを記録するために必要なアクセス許可

が引き続き付与されます。詳細については、「でサポートされているリソースタイプ AWS Config」および「に割り当てられた IAM ロールのアクセス許可 AWS Config」を参照してください。

ポリシー:「AWS_ConfigRole」ご覧ください。

AWS 管理ポリシー: AWSConfigUserAccess

この IAM ポリシーは AWS Config、リソースのタグによる検索やすべてのタグの読み取りなど、 が使用できるアクセスを提供します。これは AWS Config、管理者権限を必要とする を設定するアクセス許可を提供しません。

ポリシーを表示する: AWSConfigUserAccess。

AWS 管理ポリシー: ConfigConformsServiceRolePolicy

コンフォーマンスパックをデプロイおよび管理するには、IAM アクセス許可と他の AWS サービスからの特定のアクセス許可 AWS Config が必要です。これにより、フル機能を備えたコンフォーマンスパックをデプロイおよび管理でき、コンフォーマンスパックの新機能 AWS Config を追加するたびに更新されます。コンフォーマンスパックの詳細については、「コンフォーマンスパック」を参照してください。

ポリシー:「ConfigConformsServiceRolePolicy」ご覧ください。

AWS 管理ポリシー: AWSConfigRulesExecutionRole

AWS カスタム Lambda ルールをデプロイするには、 に IAM アクセス許可と、他の AWS サービスからの特定のアクセス許可 AWS Config が必要です。これにより、 AWS Lambda 関数は AWS Config API と、 が定期的に Amazon S3 に AWS Config 配信する設定スナップショットにアクセスできます。このアクセスは、 AWS カスタム Lambda ルールの設定変更を評価する関数で必要であり、 が新しい機能 AWS Config を追加するたびに更新されます。 AWS カスタム Lambda ルールの詳細については、AWS Config 「カスタム Lambda ルールの作成」を参照してください。設定スナップショットの詳細については、「概念 | 設定スナップショット」を参照してください。設定スナップショットの配信の詳細については、「配信チャネルの管理」を参照してください。

ポリシー:「AWSConfigRulesExecutionRole」をご覧ください。

AWS 管理ポリシー: AWSConfigMultiAccountSetupPolicy

の組織内のメンバーアカウント間で AWS Config ルールとコンフォーマンスパックを一元的にデプロイ、更新、削除するには AWS Organizations、 に IAM アクセス許可と他の AWS のサービスからの特定のアクセス許可 AWS Config が必要です。この管理ポリシーは、 AWS Config がマルチアカウン

ト設定の新しい機能を追加するたびに更新されます。詳細については、「組織内のすべてのアカウントでの AWS Config ルールの管理」および「組織内のすべてのアカウントでのコンフォーマンスパックの管理」を参照してください。

ポリシー:「AWSConfigMultiAccountSetupPolicy」をご覧ください。

AWS 管理ポリシー: AWSConfigRoleForOrganizations

が読み取り専用 AWS Organizations APIs AWS Config を呼び出すには、 には IAM アクセス許可と、他の AWS のサービスからの特定のアクセス許可 AWS Config が必要です。この管理ポリシーは、AWS Config がマルチアカウント設定の新しい機能を追加するたびに更新されます。詳細については、「組織内のすべてのアカウントでの AWS Config ルールの管理」および「組織内のすべてのアカウントでのコンフォーマンスパックの管理」を参照してください。

ポリシー:「AWSConfigRoleForOrganizations」をご覧ください。

AWS マネージドポリシー: AWSConfigRemediationServiceRolePolicy

AWS Config がユーザーに代わって`NON_COMPLIANT`リソースを修復するには、 AWS Config に IAM アクセス許可と他の AWS サービスからの特定のアクセス許可が必要です。この管理ポリシーは、修復のための新機能 AWS Config を追加するたびに更新されます。修復の詳細については、「 AWS Config ルールを使用した非準拠リソースの修復」を参照してください。可能な AWS Config 評価結果を開始する条件の詳細については、「概念 | AWS Config ルール」を参照してください。

ポリシー:「AWSConfigRemediationServiceRolePolicy」をご覧ください。

AWS ConfigAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始 AWS Config してからの の AWS 管理ポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、 AWS Config ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSConfigServiceRolePolicy – "backup-gateway:GetHypervisor" を追加します。 "backup-gateway:ListHypervisors"、 「bcm-data-exports:GetExport	このポリシーは AWS Billing and Cost Management、 AWS Backup gateway、Amazon Bedrock、 AWS CloudFormation、Amazon CloudFront、 AWS Entity Resolutio	2025 年 6 月 18 日

変更	説明	日付
」、「bcm-data-exports:ListExports」、「bcm-data-exports:ListTagsForResource」、「bedrock:GetAgent」、「bedrock:GetAgentActionGroup」、「bedrock:GetAgentKnowledgeBase」、「bedrock:GetDataSource」、「bedrock:GetFlowAlias」、「bedrock:GetFlowVersion」、「bedrock:ListAgentActionGroups」、「bedrock:ListAgentKnowledgeBases」、「bedrock:ListDataSources」、「bedrock:ListFlowAliases」、「bedrock:ListFlowVersions」、"cloudformation:BatchDescribeTypeConfigurations"、"cloudformation:DescribeStackInstance"、"cloudformation:DescribeStackSet"、"cloudformation:ListStackInstances"、"cloudformation:ListStackSets"、"cloudfront:GetPublicKey"、"cloudfront:GetRealtimeLogConfig"、"cloudfront:ListPublicKeys"、"cloudfront:ListRealtimeLogConfigs"、"entityresolution:GetIdMappingWorkflow"、"entityresolution:GetSchemaMapping"、"entityresolution:ListIdMappingWorkflows"、	n AWS IoT Core Device Advisor、 AWS Lambda、AWS Network Manager、AWS Private Certificate Authority、Amazon Relational Database Service、Amazon Redshift、Amazon S3 Tables、 に対する追加のアクセス許可をサポートするようになりました AWS Systems Manager Quick Setup。	

変更	説明	日付
"entityresolution:ListSchemaMappings"、「entityresolution:ListTagsForResource」、"iotdeviceadvisor:GetSuiteDefinition"、"iotdeviceadvisor:ListSuiteDefinitions"、"lambda:GetEventSourceMapping"、"lambda:ListEventSourceMappings"、「mediapackagev2:GetChannel」、「mediapackagev2:ListChannels」、"networkmanager:GetTransitGatewayPeering"、"networkmanager:ListPeerings"、「pca-connector-ad:GetDirectoryRegistration」、"pca-connector-ad:ListDirectoryRegistrations"、「pca-connector-ad:ListTagsForResource」、"rds:DescribeDBShardGroups"、"rds:DescribeIntegrations"、"redshift:DescribeIntegrations"、"s3tables:GetTableBucket"、"s3tables:GetTableBucketEncryption"、"s3tables:GetTableBucketMaintenanceConfiguration"、"s3tables:ListTableBuckets"、"ssm-quicksetup:GetConfigurationManager"、「ssm-quicksetup:ListConfigurationManagers」		

変更	説明	日付
AWS_ConfigRole – "backup-gateway:GetHypervisor" を追加します。 "backup-gateway:ListHypervisors"、「bcm-data-exports:GetExport」、「bcm-data-exports:ListExports」、「bcm-data-exports:ListTagsForResource」、「bedrock:GetAgent」、「bedrock:GetAgentActionGroup」、「bedrock:GetAgentKnowledgeBase」、「bedrock:GetDataSource」、「bedrock:GetFlowAlias」、「bedrock:GetFlowVersion」、「bedrock:ListAgentActionGroups」、「bedrock:ListAgentKnowledgeBases」、「bedrock:ListDataSources」、「bedrock:ListFlowAliases」、「bedrock:ListFlowVersions」、"cloudformation:BatchDescribeTypeConfigurations"、"cloudformation:DescribeStackInstance"、 "cloudformation:DescribeStackSet"、"cloudformation:ListStackInstances"、 "cloudformation:ListStackSets"、 "cloudfront:GetPublicKey"、 "cloudfront:GetRealtimeLogConfig"、"cloudfront:ListPublicKeys"、	このポリシーは AWS Backup gateway、、Amazon Bedrock AWS Billing and Cost Management、、AWS CloudFormation Amazon CloudFront、AWS Entity Resolution AWS IoT Core Device Advisor、 AWS Lambda AWS Network Manager、AWS Private Certificate Authority、Amazon Relational Database Service、Amazon Redshift、Amazon S3 Tables、 に対する追加のアクセス許可をサポートするようになりました AWS Systems Manager Quick Setup。	2025 年 6 月 18 日

変更	説明	日付
"cloudfront:ListRealtimeLogConfigs"、 "entityresolution:GetIdMappingWorkflow"、 "entityresolution:GetSchemaMapping"、 "entityresolution:ListIdMappingWorkflows"、 "entityresolution:ListSchemaMappings"、 「entityresolution:ListTagsForResource」、 "iotdeviceadvisor:GetSuiteDefinition"、 "iotdeviceadvisor:ListSuiteDefinitions"、 "lambda:GetEventSourceMapping"、 "lambda:ListEventSourceMappings"、 "networkmanager:GetTransitGatewayPeering"、 "networkmanager:ListPeerings"、 「pca-connector-ad:GetDirectoryRegistration」、 "pca-connector-ad:ListDirectoryRegistrations"、 「pca-connector-ad:ListTagsForResource」、 "rds:DescribeDBShardGroups"、 "rds:DescribeIntegrations"、 "redshift:DescribeIntegrations"、 "s3tables:GetTableBucket"、 "s3tables:GetTableBucketEncryption"、 "s3tables:GetTableBucketMaintenanceConfiguration"、 "s3tables:ListTableBuckets"、 "ssm-quicksetup:GetConfigurationManager"、 「ssm-quic		

変更	説明	日付
ksetup:ListConfigurationManagers」		
AWS_ConfigRole – 追加: "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", "bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource"	このポリシーは、Amazon Bedrock の追加のアクセス許可をサポートするようになりました。	2025 年 5 月 27 日
AWSConfigServiceRolePolicy – 追加: "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", "bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource"	このポリシーは、Amazon Bedrock の追加のアクセス許可をサポートするようになりました。	2025 年 5 月 27 日

変更	説明	日付
AWS_ConfigRole – 追加: "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	このポリシーは AWS B2B Data Interchange、、Amazon Bedrock、AWS Clean Rooms、、AWS Database Migration Service（AWS DMS）AWS CodeConnections AWS Direct Connect、Amazon CloudWatch Logs、Amazon Macie、Amazon Managed Blockchain、Amazon Q Business、Route 53 Profiles、Amazon Simple Storage Service (Amazon S3)、Amazon SageMaker AI AWS Security Hub、および Contacts、および AWS Systems Manager Incident Manager AWS Systems Manager Incident Manager の追加のアクセス許可をサポートするようになりました AWS Systems Manager。	2025 年 4 月 8 日

変更	説明	日付
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsFor Resource", "s3:GetAccessGra ntsInstance", "s3:GetAc cessGrantsLocation", "s3:Li stAccessGrantsInstances", "s3:ListAccessGrantsLocatio ns", "sagemaker:DescribeClu ster", "sagemaker:DescribeM lflowTrackingServer", "sage maker:DescribeStudioLifecyc leConfig", "sagemaker:ListC lusters", "sagemaker:ListMlf lowTrackingServers", "sagem aker:ListStudioLifecycleCon figs", "securityhub:Describ eStandardsControls", "secur ityhub:GetEnabledStandards" , "ssm-contacts:GetContact", "ssm-contacts:GetContactCha nnel", "ssm-contacts:ListCo ntactChannels", "ssm-cont acts:ListContacts", "ssm-in cidents:GetResponsePlan", " ssm-incidents:ListResponseP lans", "ssm-incidents:ListT agsForResource", "ssm:Descr ibeInstanceInformation"		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	このポリシーは AWS B2B Data Interchange、、Amazon Bedrock、AWS Clean Rooms、、AWS Database Migration Service（AWS DMS）AWS CodeConnections AWS Direct Connect、Amazon CloudWatch Logs、Amazon Macie、Amazon Managed Blockchain、Amazon Q Business、Route 53 Profiles、Amazon Simple Storage Service (Amazon S3)、Amazon SageMaker AI AWS Security Hub、および Contacts、および AWS Systems Manager Incident Manager AWS Systems Manager Incident Manager の追加のアクセス許可をサポートするようになりました AWS Systems Manager。このポリシーは、リソースパターン「」を含めることで、すべての Amazon API Gateway ドメイン名にアクセスするアクセス許可もサポートするようになりました`arn:aws:apigateway:::/domainnames/` 。	2025 年 4 月 8 日

変更	説明	日付
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation"		
AWS_ConfigRole – 追加: "ec2:GetAllowedImagesSettings"	このポリシーは、Amazon Elastic Compute Cloud (Amazon EC2) の追加のアクセス許可をサポートするようになりました。	2025 年 3 月 4 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "ec2:GetAllowedImagesSettings"	このポリシーは、Amazon Elastic Compute Cloud (Amazon EC2) の追加のアクセス許可をサポートするようになりました。	2025 年 3 月 4 日
AWS_ConfigRole – 追加: "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	このポリシーは AWS Clean Rooms、Amazon Comprehend、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Simple Storage Service (Amazon S3) AWS HealthOmics、Amazon Simple Email Service (Amazon SES) に対する追加のアクセス許可をサポートするようになりました。	2025 年 1 月 16 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	このポリシーは AWS Clean Rooms、Amazon Comprehend、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Simple Storage Service (Amazon S3) AWS HealthOmics、Amazon Simple Email Service (Amazon SES) に対する追加のアクセス許可をサポートするようになりました。	2025 年 1 月 16 日
AWSConfigServiceRolePolicy – 追加: "organizations:ListAWSServiceAccessForOrganization"	このポリシーは、 の追加のアクセス許可をサポートするようになりました AWS Organizations。	2024 年 12 月 18 日

変更	説明	日付
AWS_ConfigRole – 追加: "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", "iot:ListThingGroups", "iot	このポリシーは AWS AppConfig、、 AWS CloudTrail Amazon Connect、Amazon DataZone、Amazon DevOpsGuru、 AWS Glue Identity Store、 AWS IoT AWS IoT FleetWise、Amazon Interactive Video Service (Amazon IVS) AWS IoT Wireless、Amazon CloudWatch Logs、Amazon CloudWatch Observability Access Manager、 AWS Payment Cryptography、Amazon Relational Database Service (Amazon RDS)、Amazon Rekognition、Amazon Simple Storage Service (Amazon S3)、Amazon EventBridge Scheduler AWS Systems Manager、Amazon VPC Lattice に対する追加のアクセス許可をサポートするようになりました。	2024 年 11 月 7 日

変更	説明	日付
:ListThingTypes", "iotfleetwise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManifest", "iotfleetwise:GetSignalCatalog", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderManifestNetworkInterfaces", "iotfleetwise:ListDecoderManifests", "iotfleetwise:ListDecoderManifestSignals", "iotfleetwise:ListFleets", "iotfleetwise:ListModelManifestNodes", "iotfleetwise:ListModelManifests", "iotfleetwise:ListSignalCatalogNodes", "iotfleetwise:ListSignalCatalogs", "iotfleetwise:ListTagsForResource", "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfile", "iotwireless:GetWirelessGateway", "iotwireless:ListDestinations", "iotwireless:ListDeviceProfiles", "iotwireless:ListWirelessGateways", "ivschat:GetLoggingConfiguration", "ivschat:GetRoom" "ivschat:ListLoggingConfigurations", "ivschat:ListRooms", "ivschat:ListTagsForResource", "logs:GetLogAnomalyDetector", "logs:ListLogAnomalyDetectors", "oam:GetS		

変更	説明	日付
ink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType",	このポリシーは AWS AppConfig、、 AWS CloudTrail Amazon Connect、Amazon DataZone、Amazon DevOpsGuru、 AWS Glue Identity Store、 AWS IoT AWS IoT FleetWise、Amazon Interactive Video Service (Amazon IVS) AWS IoT Wireless、Amazon CloudWatch Logs、Amazon CloudWatch Observability Access Manager、 AWS Payment Cryptography、Amazon Relational Database Service (Amazon RDS)、Amazon Rekognition、Amazon Simple Storage Service (Amazon S3)、Amazon EventBridge Scheduler AWS Systems Manager、Amazon VPC Lattice に対する追加のアクセス許可をサポートするようになりました。	2024 年 11 月 7 日

変更	説明	日付
"iot:ListThingGroups", "iot:ListThingTypes", "iotfleetwise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManifest", "iotfleetwise:GetSignalCatalog", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderManifestNetworkInterfaces", "iotfleetwise:ListDecoderManifests", "iotfleetwise:ListDecoderManifestSignals", "iotfleetwise:ListFleets", "iotfleetwise:ListModelManifestNodes", "iotfleetwise:ListModelManifests", "iotfleetwise:ListSignalCatalogNodes", "iotfleetwise:ListSignalCatalogs", "iotfleetwise:ListTagsForResource", "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfile", "iotwireless:GetWirelessGateway", "iotwireless:ListDestinations", "iotwireless:ListDeviceProfiles", "iotwireless:ListWirelessGateways", "ivschat:GetLoggingConfiguration", "ivschat:GetRoom" "ivschat:ListLoggingConfigurations", "ivschat:ListRooms", "ivschat:ListTagsForResource", "logs:GetLogAnomalyDetector", "logs:ListLogAn		

変更	説明	日付
omalyDetectors", "oam:GetSink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

変更	説明	日付
AWS_ConfigRole – 追加: "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	このポリシーは、Amazon OpenSearch Service Severless、Amazon AppStream AWS Backup、AWS CloudTrail、 AWS Glue EC2 Image Builder、 AWS IoT Amazon Interactive Video Service (Amazon IVS) AWS Elemental MediaConnect、AWS Elemental MediaTailor AWS HealthOmics、および Amazon EventBridge スケジューラに対する追加のアクセス許可をサポートするようになりました。	2024 年 9 月 16 日

変更	説明	日付
rictionPolicies," "ivs:ListStages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	このポリシーは、Amazon OpenSearch Service Severless、Amazon AppStream AWS Backup、AWS CloudTrail、 AWS Glue EC2 Image Builder、 AWS IoT Amazon Interactive Video Service (Amazon IVS) AWS Elemental MediaConnect、AWS Elemental MediaTailor AWS HealthOmics、および Amazon EventBridge スケジューラに対する追加のアクセス許可をサポートするようになりました。	2024 年 9 月 16 日

変更	説明	日付
rictionPolicies," "ivs:ListStages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		
AWS_ConfigRole – 追加: "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	このポリシーは、Amazon Elastic File System (Amazon EFS)、Amazon Redshift、および の追加のアクセス許可をサポートするようになりました AWS Systems Manager for SAP。	2024 年 6 月 17 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	このポリシーは、Amazon Elastic File System (Amazon EFS)、Amazon Redshift、および の追加のアクセス許可をサポートするようになりました AWS Systems Manager for SAP。	2024 年 6 月 17 日

変更	説明	日付
AWS_ConfigRole – 追加: "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool," "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:G	このポリシーは、Amazon Managed Service for Prometheus、Amazon CloudWatch、Amazon Cognito、Amazon ElastiCache、Amazon FSx、 AWS Glue、 AWS Identity and Access Management (IAM) AWS Lambda、 AWS RAM、Amazon Redshift Serverless、Amazon SageMaker AI、Amazon Simple Notification Service (Amazon SNS) に対する追加のアクセス許可をサポートするようになりました。	2024 年 2 月 22 日

変更	説明	日付
etSMSSandboxAccountStatus"		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and	このポリシーは、Amazon Managed Service for Prometheus、Amazon CloudWatch、Amazon Cognito、Amazon ElastiCache、Amazon FSx、 AWS Glue、 AWS Identity and Access Management (IAM) AWS Lambda、 AWS RAM、Amazon Redshift Serverless、Amazon SageMaker AI、Amazon Simple Notification Service (Amazon SNS) に対する追加のアクセス許可をサポートするようになりました。	2024 年 2 月 22 日

変更	説明	日付
"sns:GetSMSSandboxAccountStatus"		
AWSConfigUserAccess – AWS Config この AWS 管理ポリシーの変更の追跡を開始します	このポリシーは AWS Config、リソースのタグによる検索やすべてのタグの読み取りなど、 が使用できるアクセスを提供します。これは AWS Config、管理者権限を必要とする を設定するアクセス許可を提供しません。	2024 年 2 月 22 日
AWS_ConfigRole – 追加: "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	このポリシーは AWS AppConfig、Amazon Managed Service for Prometheus、 AWS Database Migration Service（AWS DMS）、 (AWS Identity and Access Management) IAM、Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon CloudWatch Logs AWS Organizations、Amazon Simple Storage Service (Amazon S3) に対する追加のアクセス許可をサポートするようになりました。	2023 年 12 月 5 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	このポリシーは AWS AppConfig、Amazon Managed Service for Prometheus、 AWS Database Migration Service（AWS DMS）、 (AWS Identity and Access Management) IAM、Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon CloudWatch Logs AWS Organizations、Amazon Simple Storage Service (Amazon S3) に対する追加のアクセス許可をサポートするようになりました。	2023 年 12 月 5 日

変更	説明	日付
AWS_ConfigRole – 追加: "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationAssociation	このポリシーは、Amazon Cognito、Amazon Connect、Amazon EMR AWS Ground Station、AWS Mainframe Modernization、Amazon MemoryDB、AWS Organizations、Amazon QuickSight、Amazon Relational Database Service (Amazon RDS)、Amazon Redshift、Amazon Route 53 AWS Service Catalog、およびに対する追加のアクセス許可をサポートするようになりました AWS Transfer Family。	2023 年 11 月 17 日

変更	説明	日付
s," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrL		

変更	説明	日付
ocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole – 追加: "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	このポリシーにより、`AWSConfigServiceRolePolicyStatementID` 、`AWSConfigSLRLogStatementID` 、`AWSConfigSLRLogEventStatementID` 、および `AWSConfigSLRApiGatewayStatementID` のセキュリティ識別子 (SID) が追加されるようになりました。	2023 年 11 月 17 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect	このポリシーは、Amazon Cognito、Amazon Connect、Amazon EMR AWS Ground Station、AWS Mainframe Modernization、Amazon MemoryDB、AWS Organizations、Amazon QuickSight、Amazon Relational Database Service (Amazon RDS)、Amazon Redshift、Amazon Route 53 AWS Service Catalog、およびに対する追加のアクセス許可をサポートするようになりました AWS Transfer Family。	2023 年 11 月 17 日

変更	説明	日付
:ListIntegrationAssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCid		

変更	説明	日付
rBlocks," "route53:ListCidrLocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy – 追加: "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	このポリシーにより、`AWSConfigServiceRolePolicyStatementID` 、`AWSConfigSLRLogStatementID` 、`AWSConfigSLRLogEventStatementID` 、および `AWSConfigSLRApiGatewayStatementID` のセキュリティ識別子 (SID) が追加されるようになりました。	2023 年 11 月 17 日

変更	説明	日付
AWS_ConfigRole – 追加: "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListT	このポリシーは AWS Private CA、、Amazon Connect、Amazon Elastic Container Service (Amazon ECS) AWS App Mesh、Amazon CloudWatch Evidently、Amazon Managed Grafana、Amazon GuardDuty、Amazon Inspector、 AWS IoT AWS IoT TwinMaker、Amazon Managed Streaming for Apache Kafka (Amazon MSK) AWS Lambda、、AWS Network Manager AWS Organizations、および Amazon SageMaker AI に対する追加のアクセス許可をサポートするようになりました。	2023 年 10 月 4 日

変更	説明	日付
ags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSi	このポリシーは AWS Private CA、、Amazon Connect、Amazon Elastic Container Service (Amazon ECS) AWS App Mesh、Amazon CloudWatch Evidently、Amazon Managed Grafana、Amazon GuardDuty、Amazon Inspector、 AWS IoT AWS IoT TwinMaker、Amazon Managed Streaming for Apache Kafka (Amazon MSK) AWS Lambda、、AWS Network Manager AWS Organizations、および Amazon SageMaker AI に対する追加のアクセス許可をサポートするようになりました。	2023 年 10 月 4 日

変更	説明	日付
gningConfigs," "lambda:ListTags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy – "ssm:GetParameter" の削除	このポリシーは AWS Systems Manager (Systems Manager) のアクセス許可を削除するようになりました。	2023 年 9 月 6 日

変更	説明	日付
AWS_ConfigRole – 追加: "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	このポリシーは AWS App Mesh、、 AWS CloudFormation Amazon CloudFront AWS CodeArtifact、AWS CodeBuild、Amazon Connect、 AWS Glue Amazon GuardDuty、 AWS Identity and Access Management (IAM)、Amazon Inspector、 AWS IoT AWS IoT TwinMaker、 AWS IoT Wireless、Amazon Managed Streaming for Apache Kafka、Amazon Macie、AWS Elemental MediaConnect AWS Network Manager、AWS Organizations AWS Resource Explorer、Amazon Route 53、Amazon Simple Storage Service (Amazon S3)、Amazon Simple Notification Service (Amazon SNS) に対する追加のアクセス許可をサポートするようになりました。	2023 年 7 月 28 日

変更	説明	日付
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	このポリシーは AWS App Mesh、Amazon AppStream 2.0、 AWS CloudFormation Amazon CloudFront、 AWS CodeArtifact、AWS CodeBuild Amazon Connect、 AWS Glue、Amazon GuardDuty、 AWS Identity and Access Management (IAM)、Amazon Inspector AWS IoT、 AWS IoT TwinMaker、 AWS IoT Wireless、Amazon Managed Streaming for Apache Kafka、Amazon Macie、 AWS Elemental MediaConnect AWS Network Manager、AWS Organizations AWS Resource Explorer、、Amazon Route 53、Amazon Simple Storage Service (Amazon S3)、Amazon Simple Notification Service (Amazon SNS)、Amazon EC2 Systems Manager (SSM) に対する追加のアクセス許可をサポートするようになりました。	2023 年 7 月 28 日

変更	説明	日付
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

変更	説明	日付
AWS_ConfigRole – 追加: "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	このポリシーは AWS Amplify、 に対する追加のアクセス許可をサポートするようになりました。 Amazon Connect、 AWS App Mesh、 Amazon Managed Service for Prometheus、 Amazon Athena、 AWS Batch AWS CloudFormation、 AWS CloudTrail、 AWS CodeArtifact、 Amazon CodeGuru、 AWS Directory Service、 Amazon DynamoDB、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon CloudWatch Evidently 、 AWS Organizations、 Amazon Forecast、 AWS IoT Greengrass、 AWS Ground Station、 AWS Identity and Access Management (IAM)、 Amazon Managed Streaming for Apache Kafka (Amazon MSK)Amazon Lightsail、、 Amazon CloudWatch Logs、 AWS Elemental MediaConnect、 AWS Elemental MediaTailor、 Amazon Pinpoint、 Amazon Virtual Private Cloud (Amazon VPC) Amazon Personalize、 Amazon QuickSight、 AWS Migration Hub Refactor Spaces、 Amazon Simple	2023 年 6 月 13 日

変更	説明	日付
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts",	Storage Service (Amazon S3) Amazon SageMaker AI、AWS Transfer Family。	

変更	説明	日付
"organizations:ListAccounts ForParent", "organizations:L istOrganizationalUnitsForPa rent", "organizations:ListTa gsForResource", "personal ize:DescribeDataset", "perso nalize:DescribeDatasetGroup", "personalize:DescribeSchema ", "personalize:DescribeSolu tion", "personalize:ListD atasetGroups", "personalize: ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForRe source", "quicksight:ListTe mplates", "refactor-spaces:G etEnvironment", "refactor -spaces:GetService", "refactor-spaces:ListAppl ications", "refactor-spaces: ListEnvironments", "refactor -spaces:ListServices", "s3:GetAccessPointPolic yStatusForObjectLambda", "sagemaker:DescribeDe viceFleet", "sagemake r:DescribeFeatureGroup", "sa gemaker:ListDeviceFleets", "sagemaker:ListFeatureGroup s", "sagemaker:ListModels", and "transfer:ListTags ForResource"		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast	このポリシーは AWS Amplify、 に対する追加のアクセス許可をサポートするようになりました。 Amazon Connect、 AWS App Mesh、 Amazon Managed Service for Prometheus、 Amazon Athena、 AWS Batch AWS CloudFormation、 AWS CloudTrail、 AWS CodeArtifact、 Amazon CodeGuru、 AWS Directory Service、 Amazon DynamoDB、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon CloudWatch Evidently、 AWS Organizations、Amazon Forecast、 AWS IoT Greengrass、 AWS Ground Station、 AWS Identity and Access Management (IAM)、 Amazon Managed Streaming for Apache Kafka (Amazon MSK)Amazon Lightsail、、 Amazon CloudWatch Logs、 AWS Elemental MediaConnect、 AWS Elemental MediaTailor、 Amazon Pinpoint、 Amazon Virtual Private Cloud (Amazon VPC) Amazon Personalize、 Amazon QuickSight、 AWS Migration Hub Refactor Spaces、 Amazon Simple	2023 年 6 月 13 日

変更	説明	日付
:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:ListAccounts	Storage Service (Amazon S3) Amazon SageMaker AI、AWS Transfer Family。	

変更	説明	日付
ForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	このポリシーは AWS Amplify、、 AWS App Mesh、Amazon CloudFront AWS App Runner、、Amazon Elastic Compute Cloud AWS CodeArtifact、Amazon Kendra、Amazon Macie、Amazon Route 53、Amazon SageMaker AI、、 AWS Transfer Family Amazon Pinpoint、 AWS Resilience Hub AWS Migration Hub、Amazon CloudWatch、 AWS Directory Service、および の Amazon Managed Workflows に対する追加のアクセス許可をサポートするようになりました AWS WAF。	2023 年 4 月 13 日

変更	説明	日付
ion, macie2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

変更	説明	日付
AWS_ConfigRole – 追加: amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificatio	このポリシーは AWS Amplify、、 AWS App Mesh、Amazon CloudFront AWS App Runner、、Amazon Elastic Compute Cloud AWS CodeArtifact、Amazon Kendra、Amazon Macie、Amazon Route 53、Amazon SageMaker AI、、 AWS Transfer Family Amazon Pinpoint、 AWS Resilience Hub AWS Migration Hub、Amazon CloudWatch、 AWS Directory Service、および の Amazon Managed Workflows に対する追加のアクセス許可をサポートするようになりました AWS WAF。	2023 年 4 月 13 日

変更	説明	日付
nExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstancePro	このポリシーは、Amazon AppFlow AWS App Runner、、Amazon AppStream 2.0、Amazon CloudFront、Amazon CloudWatch AWS CodeArtifact、 AWS CodeCommit、Amazon CloudWatch Evidently AWS Device Farm、Amazon Forecast AWS Ground Station、、AWS Identity and Access Management (IAM) AWS IoT、Amazon MemoryDB、Amazon Pinpoint、 AWS Network Manager AWS Panorama、Amazon Relational Database Service (Amazon RDS)、Amazon Redshift、Amazon SageMaker AI の Amazon Managed Workflows に対する追加のアクセス許可をサポートするようになりました。	2023 年 3 月 30 日

変更	説明	日付
file, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

変更	説明	日付
AWS_ConfigRole – 追加: appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig,	このポリシーは、Amazon AppFlow AWS App Runner、、Amazon AppStream 2.0、 AWS CloudFormation Amazon CloudFront、Amazon CloudWatch、 AWS CodeArtifact AWS CodeCommit AWS Device Farm、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon CloudWatch Evidently、Amazon Forecast AWS Ground Station、、 AWS Identity and Access Management (IAM) AWS IoT、、Amazon MemoryDB、Amazon Pinpoint AWS Network Manager、AWS Panorama、Amazon Relational Database Service (Amazon RDS)、Amazon Redshift、Amazon SageMaker AI の Amazon Managed Workflows に対する追加のアクセス許可をサポートするようになりました。	2023 年 3 月 30 日

変更	説明	日付
groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

変更	説明	日付
AWSConfigRulesExecutionRole – この AWS 管理ポリシーの変更の追跡 AWS Config を開始します	このポリシーにより、 AWS Lambda 関数は、定期的に Amazon S3 に AWS Config 配信される AWS Config API と設定スナップショットにアクセスできます。このアクセスは、 AWS カスタム Lambda ルールの設定変更を評価する関数で必要です。	2023 年 3 月 7 日
AWSConfigRoleForOrganizations – この AWS 管理ポリシーの変更の追跡 AWS Config を開始します	このポリシーにより、 は読み取り専用 API AWS Config を呼び出すことができます。AWS Organizations APIs	2023 年 3 月 7 日
AWSConfigRemediationServiceRolePolicy – この AWS 管理ポリシーの変更の追跡 AWS Config を開始します	このポリシーにより、 AWS Config はユーザーに代わって`NON_COMPLIANT` リソースを修復できます。	2023 年 3 月 7 日
AWSConfigServiceRolePolicy – 追加: auditmanager:GetAccountStatus	このポリシーでは、 AWS Audit Managerのアカウントの登録状態を返すアクセス許可を付与するようになりました。	2023 年 3 月 3 日
AWS_ConfigRole – 追加: auditmanager:GetAccountStatus	このポリシーでは、 AWS Audit Managerのアカウントの登録状態を返すアクセス許可を付与するようになりました。	2023 年 3 月 3 日

変更	説明	日付
AWSConfigMultiAccountSetupPolicy – この AWS 管理ポリシーの変更の追跡 AWS Config を開始します	このポリシーにより AWS Config 、 は AWS サービスを呼び出し、 を使用して組織全体にリソースをデプロイ AWS Config できます AWS Organizations。	2023 年 2 月 27 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	このポリシーは、Amazon Managed Workflows for Apache Airflow、 AWS IoT Amazon AppStream 2.0、Amazon CodeGuru Reviewer、 AWS HealthLake、Amazon Kinesis Video Streams、Amazon Application Recovery Controller (ARC)、Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm、Amazon Pinpoint、AWS Identity and Access Management (IAM)、Amazon GuardDuty、Amazon CloudWatch Logs の追加アクセス許可をサポートするようになりました。	2023 年 2 月 1 日

変更	説明	日付
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

変更	説明	日付
AWS_ConfigRole – 追加: airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	このポリシーは、Amazon Managed Workflows for Apache Airflow、 AWS IoT Amazon AppStream 2.0、Amazon CodeGuru Reviewer、 AWS HealthLake、Amazon Kinesis Video Streams、Amazon Application Recovery Controller (ARC)、Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm、Amazon Pinpoint、AWS Identity and Access Management (IAM)、Amazon GuardDuty、Amazon CloudWatch Logs の追加アクセス許可をサポートするようになりました。	2023 年 2 月 1 日

変更	説明	日付
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – 更新: config:DescribeConfigRules	セキュリティのベストプラクティスとして、このポリシーは、`config:DescribeConfigRules` に対する広範なリソースレベルのアクセス許可を削除するようになりました。	2023 年 1 月 12 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	このポリシーは、Amazon Managed Service for Prometheus、 AWS Audit Manager、 AWS Database Migration Service（AWS DMS）AWS Device Farm、AWS Directory Service Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue AWS IoT、 AWS Elemental MediaPackage、Amazon Lightsail、、AWS Network Manager、Amazon QuickSight、Amazon Application Recovery Controller (ARC) AWS Resource Access Manager、Amazon Simple Storage Service (Amazon S3)、および Amazon Timestream に対する追加のアクセス許可をサポートするようになりました。	2022 年 12 月 15 日

変更	説明	日付
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

変更	説明	日付
AWS_ConfigRole – 追加: APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	このポリシーは、Amazon Managed Service for Prometheus、 AWS Audit Manager、 AWS Database Migration Service（AWS DMS）AWS Device Farm、AWS Directory Service Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue AWS IoT、 AWS Elemental MediaPackage、Amazon Lightsail、、AWS Network Manager、Amazon QuickSight、Amazon Application Recovery Controller (ARC) AWS Resource Access Manager、Amazon Simple Storage Service (Amazon S3)、および Amazon Timestream に対する追加のアクセス許可をサポートするようになりました。	2022 年 12 月 15 日

変更	説明	日付
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: cloudformation:ListStackResources and cloudformation:ListStacks	このポリシーは、指定された AWS CloudFormation スタックのすべてのリソースの説明を返し、ステータスが指定された と一致するスタックの概要情報を返すアクセス許可を付与するようになりました StackStatusFilter。	2022 年 11 月 7 日
AWS_ConfigRole – 追加: cloudformation:ListStackResources and cloudformation:ListStacks	このポリシーは、指定された AWS CloudFormation スタックのすべてのリソースの説明を返し、ステータスが指定された と一致するスタックの概要情報を返すアクセス許可を付与するようになりました StackStatusFilter。	2022 年 11 月 7 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	このポリシーは AWS Certificate Manager、 に対する追加のアクセス許可をサポートするようになりました。 Amazon Managed Workflows for Apache Airflow AWS Amplify、 AWS AppConfig 、 Amazon Keyspaces、 Amazon CloudWatch、 Amazon Connect、 AWS Glue DataBrew、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon Elastic Kubernetes Service (Amazon EKS) Amazon EventBridge、 AWS Fault Injection Service、 Amazon Fraud Detector、 Amazon FSx、 Amazon GameLift サーバー Amazon Location Service、 AWS IoT、 Amazon Lex、Amazon Lightsail、 Amazon Pinpoint、 OpsWorks AWS Panorama、 AWS Resource Access Manager、 Amazon QuickSight、 Amazon Relational Database Service (Amazon RDS) Amazon Rekognition、 AWS RoboMaker AWS Resource Groups、、 Amazon Route 53、 Amazon Simple Storage Service (Amazon S3) AWS	2022 年 10 月 19 日

変更	説明	日付
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi	Cloud Map、、 および AWS Security Token Service。	

変更	説明	日付
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

変更	説明	日付
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

変更	説明	日付
AWS_ConfigRole – 追加: acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	このポリシーは AWS Certificate Manager、 に対する追加のアクセス許可をサポートするようになりました。 Amazon Managed Workflows for Apache Airflow AWS Amplify、 AWS AppConfig 、 Amazon Keyspaces、 Amazon CloudWatch、 Amazon Connect、 AWS Glue DataBrew、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon Elastic Kubernetes Service (Amazon EKS) Amazon EventBridge、 AWS Fault Injection Service、 Amazon Fraud Detector、 Amazon FSx、 Amazon GameLift サーバー Amazon Location Service、 AWS IoT、 Amazon Lex、Amazon Lightsail、 Amazon Pinpoint、 OpsWorks AWS Panorama、 AWS Resource Access Manager、 Amazon QuickSight、 Amazon Relational Database Service (Amazon RDS) Amazon Rekognition、 AWS RoboMaker AWS Resource Groups、、 Amazon Route 53、 Amazon Simple Storage Service (Amazon S3) AWS	2022 年 10 月 19 日

変更	説明	日付
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi	Cloud Map、、 および AWS Security Token Service。	

変更	説明	日付
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

変更	説明	日付
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: Glue::GetTable	このポリシーは、指定した AWS Glue テーブルのデータカタログ内のテーブル定義を取得するアクセス許可を付与するようになりました。	2022 年 9 月 14 日
AWS_ConfigRole – 追加 Glue::GetTable	このポリシーは、指定した AWS Glue テーブルのデータカタログ内のテーブル定義を取得するアクセス許可を付与するようになりました。	2022 年 9 月 14 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	このポリシーは、Amazon AppFlow、 Amazon CloudWatch、 Amazon CloudWatch RUM、 Amazon CloudWatch Synthetics、 Amazon Connect Customer Profiles、 Amazon Connect Voice ID、 Amazon DevOpsGuru、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon EC2 Auto Scaling、 Amazon EMR、 Amazon EventBridge、 Amazon EventBridge スキーマ、 Amazon FinSpace、 Amazon Fraud Detector、 Amazon GameLift サーバー Amazon Interactive Video Service (Amazon IVS) Amazon Managed Service for Apache Flink、 EC2 Image Builder、 Amazon Lex、Amazon Lightsail、 Amazon Location Service、 Amazon Lookout for Equipment、 Amazon Lookout for Metrics Amazon Lookout for Vision、 Amazon Managed Blockchain Amazon MQ、 Amazon Nimble StudioAmazon Pinpoint、 Amazon QuickSight、 Amazon Application Recovery Controller (ARC) Amazon	2022 年 9 月 7 日

変更	説明	日付
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Route 53 Resolver、、 Amazon Simple Storage Service (Amazon S3) Amazon SimpleDB、 Amazon Simple Email Service (Amazon SES) Amazon Timestream、 AWS AppConfig、 AWS AppSync AWS Auto Scaling、 AWS Backup、 AWS Budgets、 AWS Cost Explorer、 AWS Cloud9 AWS Directory Service、 AWS DataSync AWS Elemental MediaPackage、、 AWS Glue、 AWS IoT、 AWS IoT Analytics、 AWS IoT Events AWS IoT SiteWise、 AWS License Manager、、 AWS IoT TwinMaker AWS Lake Formation、 AWS Resilience Hub、 AWS Signer、、 および AWS Transfer Family。	

変更	説明	日付
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

変更	説明	日付
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

変更	説明	日付
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

変更	説明	日付
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

変更	説明	日付
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

変更	説明	日付
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

変更	説明	日付
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

変更	説明	日付
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

変更	説明	日付
AWS_ConfigRole – 追加: appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	このポリシーは、Amazon AppFlow、 Amazon CloudWatch、 Amazon CloudWatch RUM、 Amazon CloudWatch Synthetics、 Amazon Connect Customer Profiles、 Amazon Connect Voice ID、 Amazon DevOpsGuru、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon EC2 Auto Scaling、 Amazon EMR、 Amazon EventBridge、 Amazon EventBridge スキーマ、 Amazon FinSpace、 Amazon Fraud Detector、 Amazon GameLift サーバー Amazon Interactive Video Service (Amazon IVS) Amazon Managed Service for Apache Flink、 EC2 Image Builder、 Amazon Lex、Amazon Lightsail、 Amazon Location Service、 Amazon Lookout for Equipment、 Amazon Lookout for Metrics Amazon Lookout for Vision、 Amazon Managed Blockchain Amazon MQ、 Amazon Nimble StudioAmazon Pinpoint、 Amazon QuickSight、 Amazon Application Recovery Controller (ARC) Amazon	2022 年 9 月 7 日

変更	説明	日付
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	Route 53 Resolver、、 Amazon Simple Storage Service (Amazon S3) Amazon SimpleDB、 Amazon Simple Email Service (Amazon SES) Amazon Timestream、 AWS AppConfig、 AWS AppSync AWS Auto Scaling、 AWS Backup、 AWS Budgets、 AWS Cost Explorer、 AWS Cloud9 AWS Directory Service、 AWS DataSync AWS Elemental MediaPackage、、 AWS Glue、 AWS IoT、 AWS IoT Analytics、 AWS IoT Events AWS IoT SiteWise、 AWS License Manager、、 AWS IoT TwinMaker AWS Lake Formation、 AWS Resilience Hub、 AWS Signer、、 および AWS Transfer Family	

変更	説明	日付
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

変更	説明	日付
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

変更	説明	日付
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

変更	説明	日付
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

変更	説明	日付
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

変更	説明	日付
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

変更	説明	日付
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

変更	説明	日付
ansfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject,	このポリシーでは、Amazon Managed Workflows for Apache Airflow、 AWS IoT Amazon AppStream 2.0、Amazon CodeGuru Reviewer AWS HealthLake、Amazon Kinesis Video Streams、Amazon Application Recovery Controller (ARC)、Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm、Amazon Pinpoint、 AWS Identity and Access Management (IAM)、Amazon GuardDuty、Amazon CloudWatch Logs に対する追加のアクセス許可がサポートされるようになりました。	2023 年 2 月 1 日

変更	説明	日付
devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

変更	説明	日付
AWS_ConfigRole – 追加: airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	このポリシーは、Amazon Managed Workflows for Apache Airflow、 AWS IoT Amazon AppStream 2.0、Amazon CodeGuru Reviewer、 AWS HealthLake、Amazon Kinesis Video Streams、Amazon Application Recovery Controller (ARC)、Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm、Amazon Pinpoint、AWS Identity and Access Management (IAM)、Amazon GuardDuty、Amazon CloudWatch Logs の追加アクセス許可をサポートするようになりました。	2023 年 2 月 1 日

変更	説明	日付
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – 更新: config:DescribeConfigRules	セキュリティのベストプラクティスとして、このポリシーは、`config:DescribeConfigRules` に対する広範なリソースレベルのアクセス許可を削除するようになりました。	2023 年 1 月 12 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	このポリシーは、Amazon Managed Service for Prometheus、 AWS Audit Manager、 AWS Database Migration Service（AWS DMS）AWS Device Farm、AWS Directory Service Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue AWS IoT、 AWS Elemental MediaPackage、Amazon Lightsail、、AWS Network Manager、Amazon QuickSight、Amazon Application Recovery Controller (ARC) AWS Resource Access Manager、Amazon Simple Storage Service (Amazon S3)、および Amazon Timestream に対する追加のアクセス許可をサポートするようになりました。	2022 年 12 月 15 日

変更	説明	日付
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

変更	説明	日付
AWS_ConfigRole – 追加: APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	このポリシーは、Amazon Managed Service for Prometheus、 AWS Audit Manager、 AWS Database Migration Service（AWS DMS）AWS Device Farm、AWS Directory Service Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue AWS IoT、 AWS Elemental MediaPackage、Amazon Lightsail、、AWS Network Manager、Amazon QuickSight、Amazon Application Recovery Controller (ARC) AWS Resource Access Manager、Amazon Simple Storage Service (Amazon S3)、および Amazon Timestream に対する追加のアクセス許可をサポートするようになりました。	2022 年 12 月 15 日

変更	説明	日付
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: cloudformation:ListStackResources and cloudformation:ListStacks	このポリシーは、指定された AWS CloudFormation スタックのすべてのリソースの説明を返し、ステータスが指定された と一致するスタックの概要情報を返すアクセス許可を付与するようになりました StackStatusFilter。	2022 年 11 月 7 日
AWS_ConfigRole – 追加: cloudformation:ListStackResources and cloudformation:ListStacks	このポリシーは、指定された AWS CloudFormation スタックのすべてのリソースの説明を返し、ステータスが指定された と一致するスタックの概要情報を返すアクセス許可を付与するようになりました StackStatusFilter。	2022 年 11 月 7 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	このポリシーは AWS Certificate Manager、 に対する追加のアクセス許可をサポートするようになりました。 Amazon Managed Workflows for Apache Airflow AWS Amplify、 AWS AppConfig 、 Amazon Keyspaces、 Amazon CloudWatch、 Amazon Connect、 AWS Glue DataBrew、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon Elastic Kubernetes Service (Amazon EKS) Amazon EventBridge、 AWS Fault Injection Service、 Amazon Fraud Detector、 Amazon FSx、 Amazon GameLift サーバー Amazon Location Service、 AWS IoT、 Amazon Lex、Amazon Lightsail、 Amazon Pinpoint、 OpsWorks AWS Panorama、 AWS Resource Access Manager、 Amazon QuickSight、 Amazon Relational Database Service (Amazon RDS) Amazon Rekognition、 AWS RoboMaker AWS Resource Groups、、 Amazon Route 53、 Amazon Simple Storage Service (Amazon S3) AWS	2022 年 10 月 19 日

変更	説明	日付
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi	Cloud Map、、 および AWS Security Token Service。	

変更	説明	日付
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

変更	説明	日付
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

変更	説明	日付
AWS_ConfigRole – 追加: acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	このポリシーは AWS Certificate Manager、 に対する追加のアクセス許可をサポートするようになりました。 Amazon Managed Workflows for Apache Airflow AWS Amplify、 AWS AppConfig 、 Amazon Keyspaces、 Amazon CloudWatch、 Amazon Connect、 AWS Glue DataBrew、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon Elastic Kubernetes Service (Amazon EKS) Amazon EventBridge、 AWS Fault Injection Service、 Amazon Fraud Detector、 Amazon FSx、 Amazon GameLift サーバー Amazon Location Service、 AWS IoT、 Amazon Lex、Amazon Lightsail、 Amazon Pinpoint、 OpsWorks AWS Panorama、 AWS Resource Access Manager、 Amazon QuickSight、 Amazon Relational Database Service (Amazon RDS) Amazon Rekognition、 AWS RoboMaker AWS Resource Groups、、 Amazon Route 53、 Amazon Simple Storage Service (Amazon S3) AWS	2022 年 10 月 19 日

変更	説明	日付
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi	Cloud Map、、 および AWS Security Token Service。	

変更	説明	日付
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

変更	説明	日付
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: Glue::GetTable	このポリシーは、指定した AWS Glue テーブルのデータカタログ内のテーブル定義を取得するアクセス許可を付与するようになりました。	2022 年 9 月 14 日
AWS_ConfigRole – 追加 Glue::GetTable	このポリシーは、指定した AWS Glue テーブルのデータカタログ内のテーブル定義を取得するアクセス許可を付与するようになりました。	2022 年 9 月 14 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	このポリシーは、Amazon AppFlow、 Amazon CloudWatch、 Amazon CloudWatch RUM、 Amazon CloudWatch Synthetics、 Amazon Connect Customer Profiles、 Amazon Connect Voice ID、 Amazon DevOpsGuru、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon EC2 Auto Scaling、 Amazon EMR、 Amazon EventBridge、 Amazon EventBridge スキーマ、 Amazon FinSpace、 Amazon Fraud Detector、 Amazon GameLift サーバー Amazon Interactive Video Service (Amazon IVS) Amazon Managed Service for Apache Flink、 EC2 Image Builder、 Amazon Lex、Amazon Lightsail、 Amazon Location Service、 Amazon Lookout for Equipment、 Amazon Lookout for Metrics Amazon Lookout for Vision、 Amazon Managed Blockchain Amazon MQ、 Amazon Nimble StudioAmazon Pinpoint、 Amazon QuickSight、 Amazon Application Recovery Controller (ARC) Amazon	2022 年 9 月 7 日

変更	説明	日付
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Route 53 Resolver、、 Amazon Simple Storage Service (Amazon S3) Amazon SimpleDB、 Amazon Simple Email Service (Amazon SES) Amazon Timestream、 AWS AppConfig、 AWS AppSync AWS Auto Scaling、 AWS Backup、 AWS Budgets、 AWS Cost Explorer、 AWS Cloud9 AWS Directory Service、 AWS DataSync AWS Elemental MediaPackage、、 AWS Glue、 AWS IoT、 AWS IoT Analytics、 AWS IoT Events AWS IoT SiteWise、 AWS License Manager、、 AWS IoT TwinMaker AWS Lake Formation、 AWS Resilience Hub、 AWS Signer、、 および AWS Transfer Family。	

変更	説明	日付
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

変更	説明	日付
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

変更	説明	日付
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

変更	説明	日付
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

変更	説明	日付
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

変更	説明	日付
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

変更	説明	日付
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

変更	説明	日付
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

変更	説明	日付
AWS_ConfigRole – 追加: appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	このポリシーは、Amazon AppFlow、 Amazon CloudWatch、 Amazon CloudWatch RUM、 Amazon CloudWatch Synthetics、 Amazon Connect Customer Profiles、 Amazon Connect Voice ID、 Amazon DevOpsGuru、 Amazon Elastic Compute Cloud (Amazon EC2) Amazon EC2 Auto Scaling、 Amazon EMR、 Amazon EventBridge、 Amazon EventBridge スキーマ、 Amazon FinSpace、 Amazon Fraud Detector、 Amazon GameLift サーバー Amazon Interactive Video Service (Amazon IVS) Amazon Managed Service for Apache Flink、 EC2 Image Builder、 Amazon Lex、Amazon Lightsail、 Amazon Location Service、 Amazon Lookout for Equipment、 Amazon Lookout for Metrics Amazon Lookout for Vision、 Amazon Managed Blockchain Amazon MQ、 Amazon Nimble StudioAmazon Pinpoint、 Amazon QuickSight、 Amazon Application Recovery Controller (ARC) Amazon	2022 年 9 月 7 日

変更	説明	日付
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	Route 53 Resolver、、 Amazon Simple Storage Service (Amazon S3) Amazon SimpleDB、 Amazon Simple Email Service (Amazon SES) Amazon Timestream、 AWS AppConfig、 AWS AppSync AWS Auto Scaling、 AWS Backup、 AWS Budgets、 AWS Cost Explorer、 AWS Cloud9 AWS Directory Service、 AWS DataSync AWS Elemental MediaPackage、、 AWS Glue、 AWS IoT、 AWS IoT Analytics、 AWS IoT Events AWS IoT SiteWise、 AWS License Manager、、 AWS IoT TwinMaker AWS Lake Formation、 AWS Resilience Hub、 AWS Signer、、 および AWS Transfer Family	

変更	説明	日付
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

変更	説明	日付
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

変更	説明	日付
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

変更	説明	日付
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

変更	説明	日付
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

変更	説明	日付
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

変更	説明	日付
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

変更	説明	日付
ansfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		
AWSConfigServiceRolePolicy – 追加: datasync:ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists	このポリシーは、 のエージェント、DataSync の送信元と送信先の場所、DataSync AWS アカウントタスクのリスト AWS DataSync を返すアクセス許可、 の 1 つ以上の指定された名前空間に関連付けられている名前空間とサービスに関する AWS Cloud Map 概要情報を一覧表示するアクセス許可、 AWS アカウントおよび で利用可能なすべての Amazon Simple Email Service (Amazon SES) 連絡先リストを一覧表示するアクセス許可を付与するようになりました AWS アカウント。	2022 年 8 月 22 日

変更	説明	日付
AWS_ConfigRole – 追加: datasync:ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists	このポリシーは、 のエージェント、DataSync の送信元と送信先の場所、DataSync AWS アカウントタスクのリスト AWS DataSync を返すアクセス許可、 の 1 つ以上の指定された名前空間に関連付けられている名前空間とサービスに関する AWS Cloud Map 概要情報を一覧表示するアクセス許可、 AWS アカウントおよび で利用可能なすべての Amazon Simple Email Service (Amazon SES) 連絡先リストを一覧表示するアクセス許可を付与するようになりました AWS アカウント。	2022 年 8 月 22 日
ConfigConformsServiceRolePolicy – 追加: cloudwatch:PutMetricData	このポリシーは、メトリクスデータポイントを Amazon CloudWatch に発行する許可を付与するようになりました。	2022 年 7 月 25 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	このポリシーは、Amazon Elastic Container Service (Amazon ECS)、Amazon ElastiCache、Amazon EventBridge、Amazon FSx、Amazon Managed Service for Apache Flink、Amazon Location Service、Amazon Managed Streaming for Apache Kafka、Amazon QuickSight、Amazon Rekognition、Amazon Simple Storage Service (Amazon S3) AWS RoboMaker、Amazon Simple Email Service (Amazon SES) AWS Amplify、AWS AppConfig、、 AWS AppSync、 AWS Billing Conductor、 AWS DataSync AWS Firewall Manager、AWS IAM Identity Center 、(IAM Identity Center) AWS Glue、EC2 Image Builder、および Elastic Load Balancing に対する追加のアクセス許可をサポートするようになりました。	2022 年 7 月 15 日

変更	説明	日付
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

変更	説明	日付
ions, imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

変更	説明	日付
sso:GetInlinePolicyForPermissionSet		

変更	説明	日付
AWS_ConfigRole – 追加: amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	このポリシーは、Amazon Elastic Container Service (Amazon ECS)、Amazon ElastiCache、Amazon EventBridge、Amazon FSx、Amazon Managed Service for Apache Flink、Amazon Location Service、Amazon Managed Streaming for Apache Kafka、Amazon QuickSight、Amazon Rekognition、Amazon Simple Storage Service (Amazon S3) AWS RoboMaker、Amazon Simple Email Service (Amazon SES) AWS Amplify、AWS AppConfig、、 AWS AppSync、 AWS Billing Conductor、 AWS DataSync AWS Firewall Manager、AWS IAM Identity Center 、(IAM Identity Center) AWS Glue、EC2 Image Builder、および Elastic Load Balancing に対する追加のアクセス許可をサポートするようになりました。	2022 年 7 月 15 日

変更	説明	日付
scribeLocationS3, datasync: DescribeLocationSmb, datasync:DescribeTask, datasync: ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVersions, imagebuilder: ListCompo		

変更	説明	日付
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

変更	説明	日付
sso:GetInlinePolicyForPermissionSet		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	このポリシーは、指定された Amazon Athena データカタログを取得するアクセス許可を付与するようになりました。 で Athena データカタログを一覧表示します AWS アカウント。 および Athena ワークグループまたはデータカタログリソースに関連付けられたタグを一覧表示します。 Amazon Detective 動作グラフのリストを取得し、Detective 動作グラフのタグを一覧表示する。 特定の AWS Glue 開発エンドポイント名のリストのリソースメタデータのリストを取得します。 指定された AWS Glue 開発エンドポイントに関する情報を取得する で AWS Glue すべての開発エンドポイントを取得する AWS アカウント指定された AWS Glue セキュリティ設定を取得する すべての AWS Glue セキュリティ設定を取得する AWS Glue リソースに関連付けられたタグのリストを取得します。 指定された名前の AWS Glue ワークグループに関する情報を取得します。 アカウント内のすべての AWS Glue AWS クローラリソースの名前を取得します。 内のすべての AWS Glue	2022 年 5 月 31 日

変更	説明	日付
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	`DevEndpoint` リソースの名前を取得します。 AWS アカウント内のすべての AWS Glue ジョブリソースの名前を一覧表示します AWS アカウント。 AWS Glue メンバーアカウントの詳細を取得する アカウントで作成された AWS Glue ワークフローの名前を一覧表示します。 および アカウントで使用可能な AWS Glue ワークグループを一覧表示します。 Amazon GuardDuty フィルターの詳細を取得するには、 GuardDuty IPSet を取得する GuardDuty ThreatIntelSet を取得する GuardDuty メンバーアカウントの取得 GuardDuty フィルターのリストを取得する GuardDuty サービスの IPSetsを取得する GuardDuty サービスのタグを取得する GuardDuty サービスの ThreatIntelSets を取得します。 Amazon Macie アカウントの現在のステータスと設定を取得するには AWS Resource Access Manager (AWS RAM) リソース共有のリソースとプリンシパルの関連付けを取得し、リソース共有の詳細 AWS RAM を取得する。 Amazon Simple Email Service (Amazon SES) の既存の設定セットに関する情	

変更	説明	日付
	報を取得するには、 Amazon SES 設定セットに関連付けられているイベント送信先のリストを取得します。 および Amazon SES アカウントに関連付けられているすべての設定セットを一覧表示します。 Identity Center ディレクトリ属性のリストを取得するには、 AWS IAM Identity Center アクセス許可セットの詳細を取得する 指定された IAM Identity Center アクセス許可セットにアタッチされている IAM 管理ポリシーを取得します。 IAM Identity Center インスタンスのアクセス許可セットを取得する IAM Identity Center リソースのタグを取得します。	

変更	説明	日付
AWS_ConfigRole – 追加: athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	このポリシーは、指定された Amazon Athena データカタログを取得するアクセス許可を付与するようになりました。 で Athena データカタログを一覧表示します AWS アカウント。 および Athena ワークグループまたはデータカタログリソースに関連付けられたタグを一覧表示します。 Amazon Detective 動作グラフのリストを取得し、Detective 動作グラフのタグを一覧表示する。 特定の AWS Glue 開発エンドポイント名のリストのリソースメタデータのリストを取得します。 指定された AWS Glue 開発エンドポイントに関する情報を取得する で AWS Glue すべての開発エンドポイントを取得する AWS アカウント指定された AWS Glue セキュリティ設定を取得する すべての AWS Glue セキュリティ設定を取得する AWS Glue リソースに関連付けられたタグのリストを取得します。 指定された名前の AWS Glue ワークグループに関する情報を取得します。 アカウント内のすべての AWS Glue AWS クローラリソースの名前を取得します。 内のすべての AWS Glue	2022 年 5 月 31 日

変更	説明	日付
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	`DevEndpoint` リソースの名前を取得します。 AWS アカウント内のすべての AWS Glue ジョブリソースの名前を一覧表示します AWS アカウント。 AWS Glue メンバーアカウントの詳細を取得する アカウントで作成された AWS Glue ワークフローの名前を一覧表示します。 および アカウントで使用可能な AWS Glue ワークグループを一覧表示します。 Amazon GuardDuty フィルターの詳細を取得するには、 GuardDuty IPSet を取得する GuardDuty ThreatIntelSet を取得する GuardDuty メンバーアカウントの取得 GuardDuty フィルターのリストを取得する GuardDuty サービスの IPSetsを取得する GuardDuty サービスのタグを取得する GuardDuty サービスの ThreatIntelSets を取得します。 Amazon Macie アカウントの現在のステータスと設定を取得するには AWS Resource Access Manager (AWS RAM) リソース共有のリソースとプリンシパルの関連付けを取得し、リソース共有の詳細 AWS RAM を取得する。 Amazon Simple Email Service (Amazon SES) の既存の設定セットに関する情	

変更	説明	日付
	報を取得するには、 Amazon SES 設定セットに関連付けられているイベント送信先のリストを取得します。 および Amazon SES アカウントに関連付けられているすべての設定セットを一覧表示します。 Identity Center ディレクトリ属性のリストを取得するには、 AWS IAM Identity Center アクセス許可セットの詳細を取得する 指定された IAM Identity Center アクセス許可セットにアタッチされている IAM 管理ポリシーを取得します。 IAM Identity Center インスタンスのアクセス許可セットを取得する IAM Identity Center リソースのタグを取得します。	

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	このポリシーは、すべてまたは指定された AWS CloudTrail イベントデータストア (EDS) に関する情報の取得、すべてまたは指定された AWS CloudFormation リソースに関する情報の取得、DynamoDB Accelerator (DAX) パラメータグループまたはサブネットグループのリストの取得、アクセスする現在のリージョンのアカウントの AWS Database Migration Service（AWS DMS) レプリケーションタスクに関する情報の取得、および AWS Organizations 指定されたタイプの のすべてのポリシーのリストの取得を行うアクセス許可を付与するようになりました。	2022 年 4 月 7 日

変更	説明	日付
AWS_ConfigRole – 追加: cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	このポリシーは、すべてまたは指定された AWS CloudTrail イベントデータストア (EDS) に関する情報の取得、すべてまたは指定された AWS CloudFormation リソースに関する情報の取得、DynamoDB Accelerator (DAX) パラメータグループまたはサブネットグループのリストの取得、アクセスする現在のリージョンのアカウントの AWS Database Migration Service（AWS DMS) レプリケーションタスクに関する情報の取得、および AWS Organizations 指定されたタイプの のすべてのポリシーのリストの取得を行うアクセス許可を付与するようになりました。	2022 年 4 月 7 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	このポリシーは AWS Backup、、 AWS Batch DynamoDB Accelerator、 AWS Database Migration Service、Amazon DynamoDB、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Kubernetes Service、Amazon FSx、Amazon GuardDuty、 AWS Key Management Service AWS OpsWorks、Amazon Relational Database Service、 AWS WAF V2、Amazon WorkSpaces に対する追加のアクセス許可をサポートするようになりました。	2022 年 3 月 14 日

変更	説明	日付
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

変更	説明	日付
AWS_ConfigRole – 追加: backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	このポリシーは AWS Backup、、 AWS Batch DynamoDB Accelerator、 AWS Database Migration Service、Amazon DynamoDB、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Kubernetes Service、Amazon FSx、Amazon GuardDuty、 AWS Key Management Service AWS OpsWorks、Amazon Relational Database Service、 AWS WAF V2、Amazon WorkSpaces に対する追加のアクセス許可をサポートするようになりました。	2022 年 3 月 14 日

変更	説明	日付
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	このポリシーは、Elastic Beanstalk 環境の詳細と、指定された Elastic Beanstalk 設定セットの設定内容に関する説明の取得、OpenSearch または Elasticsearch バージョンのマップの取得、データベースに利用できる Amazon RDS オプショングループの説明、および CodeDeploy デプロイ設定に関する情報の取得を実行する許可を付与するようになりました。また、このポリシーは AWS アカウント、 にアタッチされた指定された代替連絡先の取得、AWS Organizations ポリシーに関する情報の取得、Amazon ECR リポジトリポリシーの取得、アーカイブされた AWS Config ルールに関する情報の取得、Amazon ECS タスク定義ファミリーのリストの取得、指定された子 OUs) のリスト、指定されたターゲットルート、組織単位、またはアカウントにアタッチされたポリシーのリストを取得するアクセス許可を付与するようになりました。	2022 年 2 月 10 日

変更	説明	日付
AWS_ConfigRole – 追加: elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	このポリシーは、Elastic Beanstalk 環境の詳細と、指定された Elastic Beanstalk 設定セットの設定内容に関する説明の取得、OpenSearch または Elasticsearch バージョンのマップの取得、データベースに利用できる Amazon RDS オプショングループの説明、および CodeDeploy デプロイ設定に関する情報の取得を実行する許可を付与するようになりました。また、このポリシーは AWS アカウント、 にアタッチされた指定された代替連絡先の取得、AWS Organizations ポリシーに関する情報の取得、Amazon ECR リポジトリポリシーの取得、アーカイブされた AWS Config ルールに関する情報の取得、Amazon ECS タスク定義ファミリーのリストの取得、指定された子 OUs) のリスト、指定されたターゲットルート、組織単位、またはアカウントにアタッチされたポリシーのリストを取得するアクセス許可を付与するようになりました。	2022 年 2 月 10 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	このポリシーは、Amazon CloudWatch ロググループおよびストリームを作成し、作成したログストリームにログを書き込むアクセス許可を付与するようになりました。	2021 年 12 月 15日
AWS_ConfigRole – 追加: logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	このポリシーは、Amazon CloudWatch ロググループおよびストリームを作成し、作成したログストリームにログを書き込むアクセス許可を付与するようになりました。	2021 年 12 月 15 日
AWSConfigServiceRolePolicy – 追加: es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	このポリシーは、今は Amazon OpenSearch Service (OpenSearch Service) ドメイン/ドメインの詳細を取得する権限と、特定の Amazon Relational Database Service (Amazon RDS) DB パラメータグループの詳細なパラメータリストを取得するアクセスを許可します。このポリシーは、Amazon ElastiCache のスナップショットの詳細を取得するアクセスも許可します。	2021 年 9 月 8 日

変更	説明	日付
AWS_ConfigRole – 追加: es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	このポリシーは、今は Amazon OpenSearch Service (OpenSearch Service) ドメイン/ドメインの詳細を取得する権限と、特定の Amazon Relational Database Service (Amazon RDS) DB パラメータグループの詳細なパラメータリストを取得するアクセスを許可します。このポリシーは、Amazon ElastiCache のスナップショットの詳細を取得するアクセスも許可します。	2021 年 9 月 8 日

変更	説明	日付
AWSConfigServiceRolePolicy – logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine、および AWS リソースタイプの追加のアクセス許可を追加する	このポリシーは、ロググループのタグの一覧表示、ステートマシンのタグの一覧表示、すべてのステートマシンの一覧表示を行うアクセスを許可します。このポリシーでは、ステートマシンに関する詳細を取得するアクセスを許可するようになりました。このポリシーでは、Amazon EC2 Systems Manager (SSM)、Amazon Elastic Container Registry、Amazon FSx、Amazon Data Firehose、Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon Relational Database Service (Amazon RDS)、Amazon Route 53、Amazon SageMaker AI、Amazon Simple Notification Service AWS Database Migration Service、、 AWS Global Accelerator、および に対する追加のアクセス許可もサポートされるようになりました AWS Storage Gateway。	2021 年 7 月 28 日

変更	説明	日付
AWS_ConfigRole – AWS リソースタイプに l ogs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachineと追加のアクセス許可を追加する	このポリシーは、ロググループのタグの一覧表示、ステートマシンのタグの一覧表示、すべてのステートマシンの一覧表示を行うアクセスを許可します。このポリシーでは、ステートマシンに関する詳細を取得するアクセスを許可するようになりました。このポリシーでは、Amazon EC2 Systems Manager (SSM)、Amazon Elastic Container Registry、Amazon FSx、Amazon Data Firehose、Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon Relational Database Service (Amazon RDS)、Amazon Route 53、Amazon SageMaker AI、Amazon Simple Notification Service AWS Database Migration Service、、 AWS Global Accelerator、および に対する追加のアクセス許可もサポートされるようになりました AWS Storage Gateway。	2021 年 7 月 28 日

変更	説明	日付
AWSConfigServiceRolePolicy – AWS リソースタイプのアクセス許可ssm:DescribeDocumentPermissionを追加	このポリシーは、 AWS Systems Manager ドキュメントのアクセス許可とIAM Access Analyzer に関する情報の閲覧を許可するようになりました。このポリシーは、Amazon Kinesis、Amazon ElastiCache、Amazon EMR AWS Network Firewall、Amazon Route 53、Amazon Relational Database Service (Amazon RDS) の追加 AWS リソースタイプをサポートするようになりました。これらのアクセス許可の変更により AWS Config 、 はこれらのリソースタイプをサポートするために必要な読み取り専用 APIs を呼び出すことができます。このポリシーでは、lambda-inside-vpc マネージドルールの Lambda@ AWS Config Edge 関数のフィルタリングもサポートされるようになりました。	2021 年 6 月 8 日

変更	説明	日付
AWS_ConfigRole – AWS リソースタイプのアクセス許可の追加ssm:DescribeDocumentPermissionと追加	このポリシーは、 AWS Systems Manager ドキュメントのアクセス許可とIAM Access Analyzer に関する情報の閲覧を許可するようになりました。このポリシーは、Amazon Kinesis、Amazon ElastiCache、Amazon EMR AWS Network Firewall、Amazon Route 53、Amazon Relational Database Service (Amazon RDS) の追加 AWS リソースタイプをサポートするようになりました。これらのアクセス許可の変更により AWS Config 、 はこれらのリソースタイプをサポートするために必要な読み取り専用 APIs を呼び出すことができます。このポリシーでは、lambda-inside-vpc マネージドルールの Lambda@ AWS Config Edge 関数のフィルタリングもサポートされるようになりました。	2021 年 6 月 8 日

変更	説明	日付
AWSConfigServiceRolePolicy – 追加: API Gateway に対して読み取り専用の GET 呼び出しを行う apigateway:GET アクセス許可と、Amazon S3 読み取り専用 API を呼び出す s3:GetAccessPointPolicy アクセス許可と s3:GetAccessPointPolicyStatus アクセス許可	このポリシーは、 API Gateway の AWS Config ルールをサポートするために API Gateway への読み取り専用 GET 呼び出しを AWS Config が実行できるアクセス許可を付与するようになりました。このポリシーでは、が Amazon Simple Storage Service (Amazon S3) 読み取り専用 APIs AWS Config を呼び出すためのアクセス許可も追加されます。これは、新しい`AWS::S3::AccessPoint` リソースタイプをサポートするために必要です。	2021 年 5 月 10 日
AWS_ConfigRole – 追加: API Gateway に対して読み取り専用 GET 呼び出しを行う apigateway:GET アクセス許可と、Amazon S3 読み取り専用 API を呼び出す s3:GetAccessPointPolicy アクセス許可と s3:GetAccessPointPolicyStatus アクセス許可	このポリシーは、 for API Gateway をサポートするために、 が AWS Config API Gateway への読み取り専用 GET コール AWS Config を行うことを許可するアクセス許可を付与するようになりました。このポリシーでは、が Amazon Simple Storage Service (Amazon S3) 読み取り専用 APIs AWS Config を呼び出すためのアクセス許可も追加されます。これは、新しい`AWS::S3::AccessPoint` リソースタイプをサポートするために必要です。	2021 年 5 月 10 日

変更	説明	日付
AWSConfigServiceRolePolicy – AWS リソースタイプのssm:ListDocumentsアクセス許可と追加のアクセス許可を追加する	このポリシーは、指定した AWS Systems Manager ドキュメントに関する情報を表示するアクセス許可を付与します。このポリシーでは、Amazon Elastic File System AWS Backup、Amazon ElastiCache、Amazon Simple Storage Service (Amazon S3)、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Kinesis、Amazon SageMaker AI AWS Database Migration Service、Amazon Route 53 の追加 AWS リソースタイプもサポートされるようになりました。これらのアクセス許可の変更により AWS Config 、はこれらのリソースタイプをサポートするために必要な読み取り専用 APIs を呼び出すことができます。	2021 年 4 月 1 日

変更	説明	日付
AWS_ConfigRole – AWS リソースタイプのssm:ListDocumentsアクセス許可と追加のアクセス許可を追加する	このポリシーは、指定した AWS Systems Manager ドキュメントに関する情報を表示するアクセス許可を付与します。このポリシーでは、Amazon Elastic File System AWS Backup、Amazon ElastiCache、Amazon Simple Storage Service (Amazon S3)、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Kinesis、Amazon SageMaker AI AWS Database Migration Service、Amazon Route 53 の追加 AWS リソースタイプもサポートされるようになりました。これらのアクセス許可の変更により AWS Config 、はこれらのリソースタイプをサポートするために必要な読み取り専用 APIs を呼び出すことができます。	2021 年 4 月 1 日
`AWSConfigRole` は廃止に	`AWSConfigRole` は廃止されました。交換ポリシーは `AWS_ConfigRole` です。	2021 年 4 月 1 日
AWS Config が変更の追跡を開始しました	AWS Config は、 AWS 管理ポリシーの変更の追跡を開始しました。	2021 年 4 月 1 日

に割り当てられた IAM ロールのアクセス許可 AWS Config

IAM ロールを使用すると、一連のアクセス許可を定義できます。 は、S3 バケットへの書き込み、SNS トピックへの発行、 AWS リソースの設定詳細を取得するための `Describe`または `List` API リクエストを行うために割り当てるロール AWS Config を引き受けます。IAM ロールの詳細については、「IAM ユーザーガイド」の「IAM ロール」を参照してください。

AWS Config コンソールを使用して IAM ロールを作成または更新すると、 は必要なアクセス許可 AWS Config を自動的にアタッチします。詳細については、「コンソール AWS Config で をセットアップする」を参照してください。

> **ポリシーとコンプライアンス結果**
>
> で管理される IAM ポリシーやその他のポリシーは、 がリソースの設定変更を記録するアクセス許可を持っているかどうか AWS Config に影響を与える可能性があります。 AWS Organizationsさらに、ルールはリソースの設定を直接評価し、ルールは評価の実行時にこれらのポリシーを考慮しません。有効なポリシーが、 の使用方法と一致していることを確認してください AWS Config。

目次

- IAM ロールのポリシーの作成
  - ロールへの IAM 信頼ポリシーの追加
  - S3 バケットの IAM ロールのポリシー
  - KMS キーの IAM ロールポリシー
  - Amazon SNS トピックの IAM ロールポリシー
  - 設定詳細を取得するための IAM ロールポリシー
  - S3 バケット記録のアクセス許可の管理

IAM ロールのポリシーの作成

AWS Config コンソールを使用して IAM ロールを作成すると、 は必要なアクセス許可 AWS Config を自動的にロールにアタッチします。

を使用して AWS CLI を設定している場合、 AWS Config または既存の IAM ロールを更新する場合は、ポリシーを手動で更新して、 AWS Config が S3 バケットにアクセスし、SNS トピックに発行し、リソースに関する設定の詳細を取得できるようにする必要があります。

ロールへの IAM 信頼ポリシーの追加

がロールを引き受け AWS Config 、それを使用してリソースを追跡できるようにする IAM 信頼ポリシーを作成できます。信頼されたポリシーの詳細については、「IAM ユーザーガイド」の「ロールに関する用語と概念」を参照してください。

AWS Config ロールの信頼ポリシーの例を次に示します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

上記の IAM ロールの信頼関係で `AWS:SourceAccount` 条件を使用して、特定のアカウントに代わって操作を実行するときに、この AWS IAM ロールのみとやり取りするように Config サービスプリンシパルを制限することができます。

AWS Config は、所有アカウントに代わってオペレーションを実行するときにのみ IAM ロールを引き受けるように Config サービスプリンシパルを制限する `AWS:SourceArn`条件もサポートします。AWS Config サービスプリンシパルを使用する場合、 `AWS:SourceArn`プロパティは常に に設定されます`arn:aws:config:sourceRegion:sourceAccountID:*`。ここで、 `sourceRegion` はカスタマーマネージド設定レコーダーのリージョンであり、 `sourceAccountID`はカスタマーマネージド設定レコーダーを含むアカウントの ID です。

たとえば、Config サービスプリンシパルが、アカウント の us-east-1リージョンのカスタマーマネージド設定レコーダーに代わってのみ IAM ロールを引き受けるように制限する条件を追加します123456789012"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}。

S3 バケットの IAM ロールのポリシー

次のポリシー例では、S3 バケットへのアクセス AWS Config 許可を付与します。

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

KMS キーの IAM ロールポリシー

次のポリシー例では、S3 バケット配信の新しいオブジェクトで KMS ベースの暗号化を使用する AWS Config アクセス許可を付与します。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

Amazon SNS トピックの IAM ロールポリシー

次のポリシー例では、SNS トピックにアクセスするアクセス AWS Config 許可を付与します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

SNS トピックが暗号化されている場合、追加の設定手順については、「Amazon Simple Notification Service デベロッパーガイド」の「AWS KMS アクセス許可の設定」を参照してください。

設定詳細を取得するための IAM ロールポリシー

AWS Config サービスにリンクされたロール を使用することをお勧めします`AWSServiceRoleForConfig`。サービスにリンクされたロールは事前定義されており、 が他のを呼び出す AWS Config ために必要なすべてのアクセス許可が含まれています AWS のサービス。AWS Config サービスにリンクされたロールは、サービスにリンクされた設定レコーダーに必要です。詳細については、「AWS Config用のサービスリンクロールの使用」を参照してください。

コンソールでロールを作成または更新すると、 によって AWSServiceRoleForConfig がア AWS Config タッチされます。

を使用する場合は AWS CLI、 `attach-role-policy` コマンドを使用して AWSServiceRoleForConfig の Amazon リソースネーム (ARN) を指定します。

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForConfig
```

S3 バケット記録のアクセス許可の管理

AWS Config は、S3 バケットが作成、更新、または削除されたときに通知を記録して配信します。

AWS Config サービスにリンクされたロール を使用することをお勧めします`AWSServiceRoleForConfig`。サービスにリンクされたロールは事前定義されており、 が他のを呼び出す AWS Config ために必要なすべてのアクセス許可が含まれています AWS のサービス。AWS Config サービスにリンクされたロールは、サービスにリンクされた設定レコーダーに必要です。詳細については、「AWS Config用のサービスリンクロールの使用」を参照してください。

カスタマーマネージド設定レコーダーの IAM ロールの更新

カスタマーマネージド設定レコーダーで使用される IAM ロールを更新できます。IAM ロールを更新する前に、古いロールと置き換える新しいロールを作成済みであることを確認します。設定を記録して配信チャネルに配信 AWS Config するためのアクセス許可を に付与する新しいロールにポリシーをアタッチする必要があります。

IAM ロールの作成と IAM ロールへの必要なポリシーのアタッチの詳細については、[ステップ 3: IAM ロールを作成する]を参照してください。

> **Note**
>
> 既存の IAM ロールの ARN を確認するには、IAM コンソール (https://console.aws.amazon.com/iam/) に移動します。ナビゲーションペインで [Roles] (ロール) を選択します。次に、該当するロールの名前を選択し、[Summary] (サマリ) ページの上部にある ARN を見つけます。

IAM ロールの更新

IAM ロールは、 AWS Management Console または を使用して更新できます AWS CLI。

To update the IAM role (Console)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. カスタマーマネージドレコーダータブで、設定ページで編集を選択します。
4. データガバナンスセクションで、次の IAM ロールを選択します AWS Config。
   - 既存の AWS Config サービスにリンクされたロールを使用する – 必要なアクセス許可を持つロール AWS Config を作成します。
   - アカウントからロールを選択 - [既存のロール] に対して、アカウントの IAM ロールを選択します。
5. [保存] を選択します。

To update the IAM role (AWS CLI)

put-configuration-recorderコマンドを使用して、新しいロールの Amazon リソースネーム (ARN) を指定します。

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

AWS Config 配信チャネルの Amazon S3 バケットのアクセス許可

> **Important**
>
> このページでは、 AWS Config 配信チャネルの Amazon S3 バケットをセットアップします。このページは、 AWS Config 設定レコーダーが記録できる`AWS::S3::Bucket`リソースタイプに関するものではありません。

Amazon S3 バケットとオブジェクトはデフォルトでプライベートです。バケット AWS アカウント を作成した (リソース所有者) のみがアクセス許可を持ちます。リソース所有者は、アクセスポリシーを作成することで、他のリソースやユーザーにアクセスを許可できます。

AWS Config が自動的に S3 バケットを作成すると、必要なアクセス許可が追加されます。ただし、既存の S3 バケットを指定する場合は、これらのアクセス許可を手動で追加する必要があります。

トピック

- IAM ロールの使用時に Amazon S3 バケットに必要なアクセス許可
- サービスでリンクされたロールの使用時に Amazon S3 バケットに必要なアクセス許可
- Amazon S3 バケット AWS Config へのアクセスの許可
- クロスアカウントの配信時に Amazon S3 バケットに必要なアクセス許可

IAM ロールの使用時に Amazon S3 バケットに必要なアクセス許可

AWS Config は、設定レコーダーに割り当てた IAM ロールを使用して、アカウントの S3 バケットに設定履歴とスナップショットを配信します。クロスアカウント配信の場合、 AWS Config 最初に割り当てられた IAM ロールの使用を試みます。バケットポリシーが IAM ロール`WRITE`へのアクセスを許可しない場合、 は`config.amazonaws.com`サービスプリンシパル AWS Config を使用します。バケットポリシーは、配信を完了`config.amazonaws.com`するために `WRITE`へのアクセスを許可する必要があります。配信が成功すると、 はクロスアカウント S3 バケットに配信するすべてのオブジェクトの所有権 AWS Config を維持します。

AWS Config は、設定レコーダーに割り当てた IAM ロールを使用して Amazon S3 HeadBucket API を呼び出し、S3 バケットが存在するかどうか、およびその場所を確認します。 AWS Config の確認に必要なアクセス許可がない場合は、 AWS CloudTrail ログに`AccessDenied`エラーが表示されます。ただし、 AWS Config は、S3 バケットが存在するかどうかとその場所を確認するために必要なアクセス許可がない場合でも、設定履歴とスナップショットを配信 AWS Config できます。

> **最小アクセス許可**
>
> Amazon S3 API には `s3:ListBucket`アクションが必要です。 `HeadBucket`

サービスでリンクされたロールの使用時に Amazon S3 バケットに必要なアクセス許可

AWS Config サービスにリンクされたロールには、Amazon S3 バケットにオブジェクトを配置するアクセス許可がありません。サービスにリンクされたロール AWS Config を使用して を設定する場合、 AWS Config は`config.amazonaws.com`サービスプリンシパルを使用して設定履歴とスナップショットを配信します。アカウントまたはクロスアカウント送信先の S3 バケットポリシーには、AWS Config サービスプリンシパルがオブジェクトを書き込むためのアクセス許可が含まれている必要があります。

Amazon S3 バケット AWS Config へのアクセスの許可

以下のステップを完了すると AWS Config 、 が設定履歴とスナップショットを Amazon S3 バケットに配信できるようになります。

1. S3 バケットを持つアカウント AWS Management Console を使用して にサインインします。
2. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
3. 設定項目の配信 AWS Config に使用するバケットを選択し、プロパティを選択します。
4. [Permissions] (アクセス許可) を選択します。
5. Edit Bucket Policy を選択します。
6. 次のポリシーを Bucket Policy Editor ウィンドウ内にコピーします。

> **セキュリティに関するベストプラクティス**
>
> `AWS:SourceAccount` 条件を使用してバケットポリシーでアクセスを制限することを強くお勧めします。これにより、 AWS Config が想定ユーザーに代わってのみアクセスが許可されます。

JSON

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
```

```
        }
      }
    ]
  }
```

7. バケットポリシーの以下の値を置き換えます。

   - *amzn-s3-demo-bucket* – AWS Config が設定履歴とスナップショットを配信する Amazon S3 バケットの名前。
   - *[optional] prefix* – オプションで Amazon S3 にオブジェクトキーに追加するプレフィックス。バケット内でフォルダのような構成を作成するのに役立ちます。
   - *sourceAccountID* – AWS Config が設定履歴とスナップショットを配信するアカウントの ID。
8. Save、Close の順に選択します。

`AWS:SourceAccount` 条件は、 AWS Config オペレーションを指定された に制限します AWS アカウント。単一の S3 バケットに配信する組織内のマルチアカウント設定では、サービスにリンクされたロールではなく、 AWS Organizations 条件キーで IAM ロールを使用します。例えば、`AWS:PrincipalOrgID`。詳細については、AWS Organizations 「 ユーザーガイド」の「組織のアクセス許可の管理」を参照してください。

`AWS:SourceArn` 条件は、指定された配信チャネルに AWS Config オペレーションを制限します。`AWS:SourceArn` 形式は ですarn:aws:config:*sourceRegion*:*123456789012*。

たとえば、アカウント 123456789012 の米国東部 (バージニア北部) リージョンの配信チャネルへの S3 バケットアクセスを制限するには、次の条件を追加します。

```
"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:"}
```

クロスアカウントの配信時に Amazon S3 バケットに必要なアクセス許可

別のアカウントの Amazon S3 バケットに設定履歴とスナップショットを配信するように AWS Config が設定されている場合 (クロスアカウント設定) 、配信チャネルに指定された設定レコーダーと S3 バケットが異なる場合は AWS アカウント、次のアクセス許可が必要です。

- 設定レコーダーに割り当てる IAM ロールには、 `s3:ListBucket` オペレーションを実行するための明示的なアクセス許可が必要です。これは、 がこの IAM ロールを使用して Amazon S3 HeadBucket API を AWS Config 呼び出してバケットの場所を決定するためです。

- S3 バケットポリシーには、 AWS Config サービスプリンシパルと設定レコーダーに割り当てられた IAM ロールの両方に対するアクセス許可を含める必要があります。

バケットポリシー設定の例を次に示します。

```
{
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com",
        "AWS": "IAM Role-Arn assigned to the configuration recorder"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
}
```

AWS Config 配信チャネルの KMS キーのアクセス許可

S3 バケット配信のために によって配信されるオブジェクトで KMS ベースの暗号化を使用できるようにする S3 バケットの AWS KMS キー AWS Config のポリシーを作成する場合は、このトピックの情報を使用します。

目次

- IAM ロールの使用時 (S3 バケット配信) に KMS キーに必要なアクセス許可
- サービスにリンクされたロールを使用する場合の AWS KMS キーに必要なアクセス許可 (S3 バケット配信)
- AWS KMS キー AWS Config へのアクセスの許可

IAM ロールの使用時 (S3 バケット配信) に KMS キーに必要なアクセス許可

IAM ロール AWS Config を使用して を設定する場合は、次のアクセス許可ポリシーを KMS キーにアタッチできます。

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> IAM ロール、Amazon S3 バケットポリシー、または AWS KMS キーが適切なアクセスを提供しない場合 AWS Config、設定情報を Amazon AWS Config S3 バケットに送信しようとすると失敗します。 Amazon S3 この場合、 はサービス AWS Config プリンシパルとして情報をもう一度 AWS Config 送信します。この場合、Amazon S3 バケットに情報を配信するときに AWS KMS キーを使用するための AWS Config アクセスを許可するには、以下のアクセス許可ポリシーをキーにアタッチする必要があります。

サービスにリンクされたロールを使用する場合の AWS KMS キーに必要なアクセス許可 (S3 バケット配信)

AWS Config サービスにリンクされたロールには、 AWS KMS キーにアクセスするアクセス許可がありません。したがって、サービスにリンクされたロール AWS Config を使用して を設定すると、AWS Config は代わりにサービスプリンシパルとして AWS Config 情報を送信します。以下に説明するアクセスポリシーを AWS KMS キーにアタッチして、Amazon S3 バケットに情報を配信するときに AWS KMS キーを使用する AWS Config ためのアクセスを許可する必要があります。

AWS KMS キー AWS Config へのアクセスの許可

このポリシーでは AWS Config 、Amazon S3 バケットに情報を配信するときに が AWS KMS キーを使用できるようにします。

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

キーポリシーの以下の数値を置き換えます。

- *myKMSKeyARN* – 設定項目を配信 AWS Config する Amazon S3 バケット内のデータを暗号化するために使用される AWS KMS キーの ARN。
- *sourceAccountID* – AWS Config がターゲットバケットに設定項目を配信するアカウントの ID。

上記の AWS KMS キーポリシーの `AWS:SourceAccount`条件を使用して、Config サービスプリンシパルが特定のアカウントに代わってオペレーションを実行する場合にのみ AWS KMS キーを操作するように制限できます。

AWS Config は、特定の AWS Config 配信チャネルに代わってオペレーションを実行するときに、Config サービスプリンシパルが Amazon S3 バケットとのみやり取りす

るように制限する `AWS:SourceArn`条件もサポートしています。 AWS Config サービスプリンシパルを使用する場合、 `AWS:SourceArn`プロパティは常に に設定されます`arn:aws:config:sourceRegion:sourceAccountID:*`。ここで、 `sourceRegion` は配信チャネルのリージョンであり、 `sourceAccountID`は配信チャネルを含むアカウントの ID です。 AWS Config 配信チャネルの詳細については、「配信チャネルの管理」を参照してください。たとえば、以下の条件を追加すれば、アカウント `us-east-1` の `123456789012` リージョンでの配信チャネルに代わってのみ Config サービスプリンシパルが Amazon S3 バケットと交信するように制限されます: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`。

Amazon SNS トピックへのアクセス許可

このトピックでは、別のアカウントが所有する Amazon SNS トピックを配信 AWS Config するように を設定する方法について説明します。 には、Amazon SNS トピックに通知を送信するために必要なアクセス許可 AWS Config が必要です。

AWS Config コンソールが新しい Amazon SNS トピックを作成すると、 は必要なアクセス許可 AWS Config を付与します。既存の Amazon SNS トピックを選択した場合は、Amazon SNS トピックに必要なアクセス許可が含まれ、セキュリティのベストプラクティスに従っていることを確認してください。

> **クロスリージョン Amazon SNS トピックはサポートされていません**
>
> AWS Config は現在、同じアカウント内 AWS リージョン およびアカウント間でのみアクセスをサポートしています。

目次

- IAM ロール使用時に Amazon SNS トピックに必要なアクセス許可
- サービスでリンクされたロールを使用する際 Amazon SNS トピックに必要なアクセス許可
- Amazon SNS トピック AWS Config へのアクセスの許可
- Amazon SNS トピックのトラブルシューティング

IAM ロール使用時に Amazon SNS トピックに必要なアクセス許可

アクセス許可ポリシーは、別のアカウントが所有する Amazon SNS トピックに適用できます。他のアカウントから Amazon SNS トピックを使用する場合は、既存の Amazon SNS トピックに以下のポリシーを適用します。

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

`Resource` キーの場合、*`account-id`* はトピック所有者の AWS アカウント番号です。*`account-id1`*、*`account-id2`*、および *`account-id3`* には、Amazon SNS トピックにデータを送信する AWS アカウント を使用します。*`region`* と *`myTopic`* は適切な値に置き換えることができます。

が Amazon SNS トピックに通知 AWS Config を送信すると、まず IAM ロールを使用しようとしますが、ロールまたはトピックに発行するアクセス許可がない場合、この試行 AWS アカウント は失敗します。このイベントでは、 は再度通知を送信します。今回は AWS Config サービスプリンシパル名 (SPN) として通知 AWS Config を送信します。配信が正常に実行される前に、オピックのためのアクセスポリシーは `sns:Publish` プリンシパル名に`config.amazonaws.com` アクセスを許可する必要があります。IAM ロールにトピックへの公開権限がない場合、 AWS Config に Amazon SNS トピックへのアクセスを許可するには、次のセクションで説明するアクセスポリシーを、Amazon SNS トピックにアタッチする必要があります。

サービスでリンクされたロールを使用する際 Amazon SNS トピックに必要なアクセス許可

AWS Config サービスにリンクされたロールには、Amazon SNS トピックにアクセスするアクセス許可がありません。したがって、サービスにリンクされたロール (SLR) AWS Config を使用して を設定すると AWS Config 、 は代わりにサービスプリンシパルとして AWS Config 情報を送信します。以下に説明するアクセスポリシーを Amazon SNS トピックにアタッチして、Amazon SNS トピックに情報を送信するための AWS Config アクセスを許可する必要があります。

同じアカウント設定の場合、Amazon SNS トピックと SLR が同じアカウントにあり、Amazon SNS ポリシーが SLR に「`sns:Publish`」を許可する場合、 AWS Config SPN を使用する必要はありません。以下のアクセス許可ポリシーとセキュリティのベストプラクティスの推奨事項は、クロスアカウント設定のためのものです。

Amazon SNS トピック AWS Config へのアクセスの許可

このポリシーにより AWS Config 、 は Amazon SNS トピックに通知を送信できます。別のアカウントから Amazon SNS トピック AWS Config へのアクセスを許可するには、次のアクセス許可ポリシーをアタッチする必要があります。

> **Note**
>
> セキュリティのベストプラクティスとして、 AWS Config が `AWS:SourceAccount`条件にリストされているアカウントへのアクセスを制限することによってのみ、想定ユーザーに代わって リソースにアクセスするようにすることを強くお勧めします。

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
```

```
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

Resource キーの場合、*account-id* はトピック所有者の AWS アカウント番号です。*account-id1*、*account-id2*、および *account-id3* には、Amazon SNS トピックにデータを送信する AWS アカウント を使用します。*region* と *myTopic* は適切な値に置き換えることができます。

前の Amazon SNS トピックポリシーAWS:SourceAccountの条件を使用して、特定のアカウントに代わってオペレーションを実行するときに Amazon SNS トピックとのみやり取りするように AWS Config サービスプリンシパル名 (SPN) を制限できます。

AWS Config は、特定の AWS Config 配信チャネルに代わってオペレーションを実行するときにのみ AWS Config S3 バケットとやり取りするようにサービスプリンシパル名 (SPN) を制限する AWS:SourceArn 条件もサポートしています。 AWS Config サービスプリンシパル名 (SPN) を使用する場合、 AWS:SourceArnプロパティは常に に設定されます。arn:aws:config:sourceRegion:sourceAccountID:*ここで、 sourceRegion は配信チャネルのリージョンであり、 sourceAccountIDは配信チャネルを含むアカウントの ID です。 AWS Config 配信チャネルの詳細については、「配信チャネルの管理」を参照してください。たとえば、アカウント のus-east-1リージョン の配信チャネルに代わってのみ S3 バケットを操作するように AWS Config サービスプリンシパル名 (SPN) 123456789012を制限するには、次の条件を追加します"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}。

Amazon SNS トピックのトラブルシューティング

AWS Config には、Amazon SNS トピックに通知を送信するアクセス許可が必要です。Amazon SNS トピックが通知を受信できない場合は、引き受け AWS Config ていた IAM ロールに必要なsns:Publishアクセス許可があることを確認します。

AWS Config ID とアクセスのトラブルシューティング

以下の情報は、 および IAM の使用時に発生する可能性がある一般的な問題の診断 AWS Config と修正に役立ちます。

トピック

- でアクションを実行する権限がありません AWS Config
- iam:PassRole を実行する権限がありません
- 自分の 以外のユーザーに自分の AWS Config リソース AWS アカウント へのアクセスを許可したい

でアクションを実行する権限がありません AWS Config

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

以下のエラー例は、`mateojackson` IAM ユーザーがコンソールを使用して架空の *`my-example-widget`* リソースに関する詳細情報を表示しようとしているが、架空の `config:`*`GetWidget`* 権限がないという場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

この場合、Mateo のポリシーでは、*`my-example-widget`* アクションを使用して `config:`*`GetWidget`* リソースにアクセスすることを許可するように更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して AWS Configにロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、既存のロールをそのサービスに渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して AWS Configでアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに自分の AWS Config リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- がこれらの機能 AWS Config をサポートしているかどうかを確認するには、「」を参照してくださいが IAM と AWS Config 連携する方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、「IAM ユーザーガイド」の「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

のサービスにリンクされたロールの使用 AWS Config

AWS Config は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、直接リンクされた一意のタイプの IAM ロールです AWS Config。サービスにリンクされたロールは によって事前定義 AWS Config されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 の設定 AWS Config が簡単になります。 は、サービスにリンクされたロールのアクセス許可 AWS Config を定義します。特に定義されている場合を除き、 のみがそのロールを引き受け AWS Config ることができます。定義されたアクセス許可には、信頼ポリシーとアクセス権限ポリシーが含まれ、そのアクセス権限ポリシーを他の IAM エンティティに適用することはできません。

サービスリンクロールをサポートする他のサービスについては、「IAM と連携するAWS のサービス」を参照して、サービスリンクロール列がはいになっているサービスを探してください。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい] リンクを選択してください。

のサービスにリンクされたロールのアクセス許可 AWS Config

AWS Config は AwsServiceRoleForConfig という名前のサービスにリンクされたロール AWS Config を使用します。このサービスにリンクされたロールを使用して、ユーザーに代わって他の AWS サービスを呼び出します。

AwsServiceRoleForConfig サービスにリンクされたロールは、`config.amazonaws.com`サービスを信頼してロールを引き受けます。

`AwsServiceRoleForConfig` ロールのアクセス許可ポリシーには、 AWS Config リソースの読み取り専用アクセス許可と書き込みアクセス許可、および が AWS Config サポートする他の サービスのリソースの読み取り専用アクセス許可が含まれています。AwsServiceRoleForConfig の マネージドポリシーを表示するには、「 の AWS マネージドポリシー AWS Config」を参照してください。

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの許可」を参照してください。

でサービスにリンクされたロールを使用するには AWS Config、Amazon S3 バケットと Amazon SNS トピックに対するアクセス許可を設定する必要があります。詳細についてはサービスでリンクされたロールの使用時に Amazon S3 バケットに必要なアクセス許可、サービスにリンクされたロー

ルを使用する場合の AWS KMS キーに必要なアクセス許可 (S3 バケット配信)、およびサービスでリンクされたロールを使用する際 Amazon SNS トピックに必要なアクセス許可を参照してください。

のサービスにリンクされたロールの作成 AWS Config

IAM CLI または IAM API で、`config.amazonaws.com` サービス名でサービスリンクロールを作成します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの作成」を参照してください。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

のサービスにリンクされたロールの編集 AWS Config

AWS Config では、AwsServiceRoleForConfig サービスにリンクされたロールを編集することはできません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照する可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

のサービスにリンクされたロールの削除 AWS Config

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除しようとしたときに AWS Config サービスがロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

AwsServiceRoleForConfig で使用される AWS Config リソースを削除するには

サービスにリンクされたロールを使用して、`ConfigurationRecorders` がないことを確認します。 AWS Config コンソールを使用して設定レコーダーを停止できます。記録を停止するには、[Recording is on] (記録はオン) の [Turn off] (無効) を選択します。

AWS Config API `ConfigurationRecorder`を使用して を削除できます。削除するには、`delete-configuration-recorder` コマンドを使用します。

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

サービスリンクロールを IAM で手動削除するには

IAM コンソール、IAM CLI、または IAM API を使用して、AwsServiceRoleForConfig サービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

でのインシデント対応 AWS Config

AWSでは、セキュリティが最優先事項です。 AWS クラウド責任共有モデルの一環として、 は、セキュリティの影響を受けやすい組織の要件を満たすデータセンター、ネットワーク、ソフトウェアアーキテクチャ AWS を管理します。 AWS は、 AWS Config サービス自体に関するインシデント対応を担当します。また、 AWS お客様はクラウドでセキュリティを維持する責任を共有します。つまり、ユーザーは、アクセスできる AWS ツールや機能から実装するセキュリティを制御し、責任共有モデルのユーザー側のインシデント対応に責任を負います。

クラウド上で稼働するアプリケーションの目標を満たすセキュリティベースラインを確立することで、対応可能な逸脱を検出できます。セキュリティインシデント対応は複雑なトピックになる可能性があるため、インシデント対応 (IR) と選択が企業目標に与える影響をよりよく理解できるように、セキュリティAWS インシデント対応ガイド、AWS セキュリティのベストプラクティスホワイトペーパー、 AWS クラウド導入フレームワーク (CAF) のセキュリティ視点ホワイトペーパーのリソースを確認することをお勧めします。

のコンプライアンス検証 AWS Config

サードパーティーの監査者は、複数の AWS コンプライアンスプログラムの一環として AWS Config のセキュリティとコンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、AWS のサービス 「コンプライアンスプログラムによる範囲内」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべてが HIPAA AWS のサービス の対象となるわけではありません。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) など) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – 不審なアクティビティや悪意のあるアクティビティがないか環境をモニタリングすることで AWS アカウント、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性 AWS Config

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

のインフラストラクチャセキュリティ AWS Config

マネージドサービスである AWS Config は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS が公開した API コールを使用して、ネットワーク AWS Config 経由で にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードはJava 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。またはAWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

設定と脆弱性の分析

では AWS Config、ゲストオペレーティングシステム (OS) やデータベースのパッチ適用、ファイアウォール設定、ディザスタリカバリなどの基本的なセキュリティタスク AWS を処理します。

サービス間の混乱した代理の防止

混乱した代理問題は、アクションを実行する許可を持たないエンティティが、より特権のあるエンティティにアクションを実行するように強制できるセキュリティの問題です。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、 AWS では、アカウントのリソースへのアクセス権が付与されたサービスプリンシパルで、すべてのサービスのデータを保護するために役立つツールを提供しています。

リソースポリシーで `aws:SourceArn`および `aws:SourceAccount` グローバル条件コンテキストキーを使用して、 がリソースに別のサービス AWS Config に付与するアクセス許可を制限することをお勧めします。クロスサービスアクセスにリソースを 1 つだけ関連付けたい場合は、`aws:SourceArn` を使用します。そのアカウント内のリソースをクロスサービスの使用に関連付けることを許可する場合は、`aws:SourceAccount` を使用します。

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して、`aws:SourceArn` グローバル条件コンテキストキーを使用することです。リソースの完全な ARN が不明な場合や、複数のリソースを指定する場合には、グローバルコンテキスト条件キー `aws:SourceArn` で、ARN の未知部分を示すためにワイルドカード文字 (*) を使用します。例えば、`arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`。

`aws:SourceArn` の値に Amazon S3 バケット ARN などのアカウント ID が含まれていない場合は、両方のグローバル条件コンテキストキーを使用して、アクセス許可を制限する必要があります。

次の例は、 で `aws:SourceArn`および `aws:SourceAccount` グローバル条件コンテキストキーを使用して、混乱した代理問題 AWS Config を防ぐ方法を示しています。Amazon S3 バケット AWS Config へのアクセスを許可する。

のセキュリティのベストプラクティス AWS Config

AWS Config には、独自のセキュリティポリシーを開発および実装する際に考慮すべき多くのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを説明するものではありません。これらのベストプラクティスはお客様の環境に適切ではないか、十分ではない場合があるため、これらは指示ではなく、有用な考慮事項と見なしてください。

- のタグ付けを活用することで AWS Config、 リソースの管理、検索、フィルタリングが容易になります。
- 配信チャネルが正しく設定されていることを確認し、確認したら、 が正しく記録 AWS Config されていることを確認します。

詳細については、AWS Config ベストプラクティスのブログを参照してください。

でのログ記録とモニタリング AWS Config

AWS Config は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています AWS Config。モニタリングは、 および AWS Config AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。

トピック

- を使用した AWS Config API コールのログ記録 AWS CloudTrail
- モニタリング

を使用した AWS Config API コールのログ記録 AWS CloudTrail

CloudTrail は、 のすべての API コールをイベント AWS Config としてキャプチャします。キャプチャされた呼び出しには、 AWS Config コンソールからの呼び出しと AWS Config API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、イベントを含む Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます AWS Config。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、リクエストの実行元の IP アドレス AWS Config、リクエストの実行者、リクエストの実行日時などの詳細を確認できます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

トピック

- AWS Config CloudTrail の情報
- AWS Config ログファイルエントリについて
- ログファイルの例

AWS Config CloudTrail の情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。アクティビティが発生すると AWS Config、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、CloudTrail イベント履歴でのイベントの表示を参照してください。

のイベントなど AWS アカウント、 のイベントの継続的な記録については AWS Config、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 複数のリージョンから CloudTrail ログファイルを受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

すべての AWS Config オペレーションは CloudTrail によってログに記録され、 AWS Config API リファレンスに記載されています。例えば、DeliverConfigSnapshot、DeleteDeliveryChannel、および DescribeDeliveryChannels などのオペレーションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

AWS Config ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

ログファイルの例

CloudTrail ログエントリの例については、以下のトピックを参照してください。

DeleteDeliveryChannel

次の例は、DeleteDeliveryChannel オペレーションのCloudTrail ログファイルです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DeliverConfigSnapshot

次の例は、 DeliverConfigSnapshot オペレーションの CloudTrail ログエントリです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
```

```
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

DescribeConfigurationRecorderStatus

次の例は、DescribeConfigurationRecorderStatus オペレーションの CloudTrail ログファイルです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

次の例は、DescribeConfigurationRecorders オペレーションの CloudTrail ログファイルです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
```

```
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

次の例は、DescribeDeliveryChannels オペレーションの CloudTrail ログファイルです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

次の例は、GetKeyPolicy オペレーションの CloudTrail ログファイルです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
```

```
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```

PutConfigurationRecorder

次の例は、PutConfigurationRecorder オペレーションの CloudTrail ログファイルです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
```

```
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

以下の例は、PutDeliveryChannel オペレーションの CloudTrail ログファイルです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
```

```
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

次の例は、StartConfigurationRecorder オペレーションの CloudTrail ログファイルです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
```

```
    }
```

StopConfigurationRecorder

次の例は、StopConfigurationRecorder オペレーションの CloudTrail ログファイルです。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

モニタリング

他の AWS サービスを使用してリソースをモニタリングできます AWS Config 。

- Amazon Simple Notification Service (SNS) を使用すると、ユーザー API アクティビティの結果としてサポートされている AWS リソースが作成、更新、またはその他の方法で変更されるたびに通知を送信できます。
- Amazon EventBridge を使用して、 AWS Config イベントのステータスでの変更を検出し、対応できます。

トピック

- Amazon SQS による AWS リソース変更のモニタリング
- Amazon EventBridge AWS Config によるモニタリング

Amazon SQS による AWS リソース変更のモニタリング

AWS Config は Amazon Simple Notification Service (SNS) を使用して、ユーザー API アクティビティの結果としてサポートされている AWS リソースが作成、更新、またはその他の方法で変更されるたびに通知を送信します。ただし、特定のリソースの設定変更以外の情報は必要ない場合もあります。例えば、第三者によるセキュリティグループの設定変更を知ることは重要であっても、Amazon EC2 インスタンスのタグの変更を逐一知る必要はないでしょう。または、特定のリソースの更新時に特定のアクションを実行するプログラムを記述する場合があります。例えば、セキュリティグループの設定の変更時に、特定のワークフローを開始する場合があります。これらの方法で からのデータをプログラム AWS Config で使用する場合、Amazon SNS の通知エンドポイントとして Amazon Simple Queue Service キューを使用します。

> **Note**
>
> 通知は、Amazon SNS から E メール、SMS 対応の携帯電話やスマートフォンに対するショートメッセージサービス (SMS) のメッセージ、モバイルデバイスのアプリケーションに対する通知メッセージ、または 1 つ以上の HTTP や HTTPS エンドポイントに対する通知メッセージの形式で着信する場合があります。

リージョンごとに 1 つのトピックがある場合であれ、各リージョンでアカウントごとに 1 つのトピックがある場合であれ、1 つの SQS キューを複数のトピックにサブスクライブできます。キューは目的の SNS トピックにサブスクライブする必要があります (複数のキューを 1 つの SNS トピックにサブスクライブできます)。詳細については、Amazon SQS キューへの Amazon SNS メッセージの送信を参照してください。

Amazon SQS のアクセス許可

で Amazon SQS を使用するには AWS Config、SQS キューで許可されているすべてのアクションを実行するためのアクセス許可をアカウントに付与するポリシーを設定する必要があります。以下のポリシー例では、アカウント番号 111122223333 とアカウント番号 444455556666 に対して、各設定変更に関するメッセージを arn:aws:sqs:us-east-2:444455556666:queue1 という名前のキューを送信するためのアクセス許可を付与します。

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

SNS トピックとそのトピックにサブスクライブする SQS キューの間の接続に対してアクセス許可を付与するポリシーを作成する必要もあります。次のポリシー例では、Amazon リソースネーム (ARN) が arn:aws:sns:us-east-2:111122223333:test-topic である SNS トピックに対して、arn:aws:sqs:us-east-2:111122223333:test-topic-queue という名前のキューにアクションを実行することを許可します。

> **Note**
>
> SQS キューと SNS トピックのアカウントは同じリージョンに存在する必要があります。

JSON

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

各ポリシーには、複数のキューではなく、1 つのキューだけを対象とするステートメントを含めることができます。Amazon SQS ポリシーに関するその他の制限については、Amazon SQS ポリシーに関する特別情報を参照してください。

Amazon EventBridge AWS Config によるモニタリング

Amazon EventBridge は、 AWS リソースの変更を記述したシステムイベントのストリームをほぼリアルタイムに配信します。Amazon EventBridge を使用して、 AWS Config イベントのステータスの変化を検出して対応します。

状態の遷移があると実行されるルールや、関心のある 1 以上の遷移があると実行されるルールを作成できます。次に、ユーザーが作成するルールに基づいて、ルール内のユーザー指定の値にイベントが一致するときに、Amazon EventBridge が 1 つ、または複数のターゲットアクションを呼び出します。イベントのタイプに応じて、通知の送信、イベント情報の取得、是正措置の実施、またはその他の対策を行うことができます。

ただし AWS Config、 のイベントルールを作成する前に、以下を実行する必要があります。

- EventBridge のイベント、ルール、ターゲットに精通しておいてください。詳細については、「Amazon EventBridge とは?」を参照してください。
- EventBridge の使用を開始してルールを設定する方法の詳細については、「Amazon EventBridge の開始方法」を参照してください。
- イベントのルールで使用するターゲットを作成します。

トピック

- 考慮事項
- の Amazon EventBridge 形式 AWS Config
- AWS Config向けの Amazon EventBridge ルールの作成

考慮事項

次のリソースタイプを記録していない場合、EventBridge を通じてアラートを受け取ることはありません AWS Config。

- `AWS::ACM::Certificate`
- `AWS::CloudTrail::Trail`
- `AWS::CloudWatch::Alarm`
- `AWS::EC2::CustomerGateway`
- `AWS::EC2::EIP`
- `AWS::EC2::Host`
- `AWS::EC2::Instance`
- `AWS::EC2::InternetGateway`
- `AWS::EC2::NetworkAcl`
- `AWS::EC2::NetworkInterface`
- `AWS::EC2::RouteTable`
- `AWS::EC2::SecurityGroup`
- `AWS::EC2::Subnet`
- `AWS::EC2::VPC`
- `AWS::EC2::VPNConnection`
- `AWS::EC2::VPNGateway`
- `AWS::EC2::Volume`
- `AWS::ElasticLoadBalancingV2::LoadBalancer`
- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`

- AWS::IAM::User
- AWS::RDS::DBInstance
- AWS::RDS::DBSecurityGroup
- AWS::RDS::DBSnapshot
- AWS::RDS::DBSubnetGroup
- AWS::RDS::EventSubscription
- AWS::Redshift::Cluster
- AWS::Redshift::ClusterParameterGroup
- AWS::Redshift::ClusterSecurityGroup
- AWS::Redshift::ClusterSnapshot
- AWS::Redshift::ClusterSubnetGroup
- AWS::Redshift::EventSubscription
- AWS::S3::Bucket

の Amazon EventBridge 形式 AWS Config

の EventBridge イベント AWS Config は、次の形式です。

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

AWS Config向けの Amazon EventBridge ルールの作成

AWS Configによって出力されたイベントでトリガーする EventBridge ルールを作成するには、以下の手順を実行します。イベントはベストエフォートベースで発生します。

1. ナビゲーションペインで [ルール] を選択します。
2. [ルールの作成] を選択します。
3. ルールの名前と説明を入力します。

   ルールには同じリージョン内および同じイベントバス上の別のルールと同じ名前を付けることはできません。

   > **Note**
   >
   > イベントバスはソースからイベントを受信し、ルールを使用してイベントを評価し、設定された入力変換を適用して、適切なターゲット (複数可) にルーティングします。アカウントのデフォルトのイベントバスは、 からイベントを受信します AWS のサービス。カスタムイベントバスは、カスタムアプリケーションとサービスからイベントを受信できます。パートナーイベントバスは、SaaS パートナーによって作成されたイベントソースからイベントを受信します。これらのイベントは、パートナーサービスまたはアプリケーションから発生します。詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge のイベントバス」を参照してください。 EventBridge

4. [ルールタイプ] で、[イベントパターンを持つルール] を選択してください。
5. [Event source] (イベントソース) で、[AWS events or EventBridge partner events] (イベントまたは EventBridge パートナーイベント) を選択してください。
6. (オプション) [サンプルイベントタイプ] では、[AWS イベント] を選択します。
7. (オプション) [サンプルイベント] で、ルールをトリガーするイベントタイプを選択します。
   - [CloudTrail 経由のAWS API コール] を選択して、このサービスに対して行われた API コールをルールのベースにします。このタイプのルールの作成の詳細については、「チュートリアル: AWS CloudTrail API コール用の Amazon EventBridge ルールを作成する」を参照してください。
   - アカウント内のリソースが変更されたときに通知を受け取るには、[Config Configuration Item Change] (設定項目の変更) を選択します。

     これらのサポート記事で説明されているように、EventBridge を使用して、リソースが作成または削除されたときにカスタム E メール通知を受け取ることができます。 AWS Config サービ

ス AWS アカウント を使用して でリソースが作成されたときにカスタム E メール通知を受け取るにはどうすればよいですか？ および AWS Config サービス AWS アカウント を使用して でリソースが削除されたときにカスタム E メール通知を受け取るにはどうすればよいですか？

- ルールに対するコンプライアンスチェックが失敗したときに通知を受け取るには、[Config Rules Compliance Change] (設定ルールのコンプライアンス変更) を選択します。

  このサポート記事で説明されているように、EventBridge を使用して、リソースが準拠していない場合にカスタム E メール通知を受信できます。 を使用して AWS リソースが準拠していない場合に通知を受け取るにはどうすればよいですか AWS Config？

- 再評価ステータスの通知を受け取るには、[Config Rules Re-evaluation Status] (設定ルールの再評価ステータス) を選択します。
- 設定スナップショットの配信ステータスの通知を受け取るには、[Config Configuration Snapshot Delivery Status] (設定スナップショット配信ステータス) を選択します。
- 設定履歴の配信ステータスの通知を受け取るには、[Config Configuration History Delivery Status] (設定スナップショット履歴の配信ステータス) を選択します。

8. 作成方法 では、パターンフォームの使用 を選択します。
9. [イベントソース] で、[AWS のサービス] を選択してください。
10. [AWS サービス名] には [Config] を選択します。
11. [イベントタイプ] で、ルールをトリガーするイベントタイプを選択します。

- すべてのイベントを選択して、すべての AWS サービスに適用されるルールを作成します。このオプションを選択した場合、特定のメッセージタイプ、ルール名、リソースタイプ、またはリソース ID を選択することはできません。
- [CloudTrail 経由のAWS API コール] を選択して、このサービスに対して行われた API コールをルールのベースにします。このタイプのルールの作成の詳細については、「チュートリアル: AWS CloudTrail API コール用の Amazon EventBridge ルールを作成する」を参照してください。
- アカウント内のリソースが変更されたときに通知を受け取るには、[Config Configuration Item Change] (設定項目の変更) を選択します。

  これらのサポート記事で説明されているように、EventBridge を使用して、リソースが作成または削除されたときにカスタム E メール通知を受け取ることができます。 AWS Config サービス AWS アカウント を使用して でリソースが作成されたときにカスタム E メール通知を受け取るにはどうすればよいですか？ および AWS Config サービス AWS アカウント を使用して でリソースが削除されたときにカスタム E メール通知を受け取るにはどうすればよいですか？

- ルールに対するコンプライアンスチェックが失敗したときに通知を受け取るには、[Config Rules Compliance Change] (設定ルールのコンプライアンス変更) を選択します。

  このサポート記事で説明されているように、EventBridge を使用して、リソースが準拠していない場合にカスタム E メール通知を受信できます。 を使用して AWS リソースが準拠していない場合に通知を受け取るにはどうすればよいですか AWS Config？
- 再評価ステータスの通知を受け取るには、[Config Rules Re-evaluation Status] (設定ルールの再評価ステータス) を選択します。
- 設定スナップショットの配信ステータスの通知を受け取るには、[Config Configuration Snapshot Delivery Status] (設定スナップショット配信ステータス) を選択します。
- 設定履歴の配信ステータスの通知を受け取るには、[Config Configuration History Delivery Status] (設定スナップショット履歴の配信ステータス) を選択します。

12. 任意のタイプの通知を受け取るには、[Any message type] (任意のメッセージタイプ) を選択します。次のタイプの通知を受け取るには、[Specific message type(s)] (特定のメッセージタイプ) を選択します。
    - ConfigurationItemChangeNotification を選択すると、 が AWS Config 評価するリソースの設定が変更されると、メッセージが表示されます。
    - ComplianceChangeNotification を選択した場合、 AWS Config が評価するリソースタイプが変更されたときに、メッセージを受け取ります。
    - ConfigRulesEvaluationStarted を選択すると、 が指定されたリソースに対してルールの評価 AWS Config を開始すると、メッセージが表示されます。
    - ConfigurationSnapshotDeliveryCompleted を選択すると、 が設定スナップショットを Amazon S3 バケットに AWS Config 正常に配信すると、メッセージが表示されます。
    - ConfigurationSnapshotDeliveryFailed を選択すると、 AWS Config が設定スナップショットを Amazon S3 バケットに配信できなかったときにメッセージが表示されます。
    - ConfigurationSnapshotDeliveryStarted を選択すると、 が設定スナップショットを Amazon S3 バケットに配信 AWS Config し始めたときにメッセージが表示されます。
    - ConfigurationHistoryDeliveryCompleted を選択すると、 が設定履歴を Amazon S3 バケットに AWS Config 正常に配信すると、メッセージが表示されます。
13. イベントタイプのドロップダウンリストから特定のイベントタイプを選択した場合は、任意のリソースタイプを選択して、 AWS Config サポートされているすべてのリソースタイプに適用されるルールを作成します。

    または、[Specific resource type(s)] (特定のリソースタイプ) を選択し、サポートされる AWS Config リソースタイプ (例: `AWS::EC2::Instance`) を入力します。

14. [Event Type] (イベントタイプ) ドロップダウンリストから特定のイベントタイプを選択した場合は、[Any resource ID] (任意のリソース ID) を選択して、サポートされる AWS Config リソース ID を含めます。

    または、[Specific resource ID(s)] (特定のリソース ID) を選択し、サポートされる AWS Config リソース ID (例: `i-04606de676e635647`) を入力します。
15. [Event Type] (イベントタイプ) ドロップダウンリストから特定のイベントタイプを選択した場合は、[Any rule name] (任意のルール名) を選択して、サポートされる AWS Config ルールを含めます。

    または、[Specific rule name(s)] (特定のルール名) を選択し、サポートされる AWS Config ルール (例: required-tags) を入力します。
16. [ターゲットの選択] で、このルールでの使用のために準備したターゲットのタイプを選択してから、そのタイプに必要な追加のオプションを設定します。
17. 表示されるフィールドは、選択したサービスによって異なります。必要に応じて、このターゲットタイプに固有の情報を入力します。
18. 多くのターゲットタイプでは、EventBridge はターゲットにイベントを送信するためのアクセス許可が必要です。これらの場合、EventBridge は、イベントの実行に必要な IAM ロールを作成できます。
    - 自動的に IAM ロールを作成するには、[Create a new role for this specific resource (この特定のリソースに対して新しいロールを作成する)] を選択します。
    - 以前に作成した IAM ロールを使用するには、[Use existing role (既存のロールの使用)] を選択します。
19. (オプション) [Add target (ターゲットの追加)] を選択して、このルールに別のターゲットを追加します。
20. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、「Amazon EventBridge のタグ」を参照してください。
21. ルール設定を確認して、イベントモニタリング要件を満たしていることを確認します。
22. [Create] (作成) を選択して、選択を確定します。

インターフェイス Amazon VPC エンドポイント AWS Config での の使用

Amazon Virtual Private Cloud (Amazon VPC) を使用して AWS リソースをホストする場合は、VPC と の間にプライベート接続を確立できます AWS Config。この接続を使用すると、パブリックインターネットを経由せずに、VPC から AWS Config と通信できます。

Amazon VPC は、定義した仮想ネットワークで AWS リソースを起動するために使用できる AWS サービスです。VPC を使用することで、IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどのネットワーク設定を制御できます。インターフェイス VPC エンドポイントは、プライベート IP アドレスを持つ Elastic Network Interface を使用して AWS サービス間のプライベート通信を可能にする AWS テクノロジーである AWS PrivateLink を利用しています。VPC を接続するには AWS Config、インターフェイス VPC エンドポイントを定義します AWS Config。このタイプのエンドポイントを使用すると、VPC を AWS サービスに接続できます。エンドポイントは、インターネットゲートウェイ、ネットワークアドレス変換 (NAT) インスタンス、または VPN 接続を必要と AWS Config せずに、信頼性が高くスケーラブルな への接続を提供します。詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC とは」を参照してください。

以下の手順は、Amazon VPC のユーザー向けです。詳細については、『Amazon VPC ユーザーガイド』の「開始方法」を参照してください。

の VPC エンドポイントを作成する AWS Config

VPC AWS Config で の使用を開始するには、インターフェイス VPC エンドポイントを作成します AWS Config。の設定を変更する必要はありません AWS Config。 は、パブリックエンドポイントを使用して他の AWS サービスを AWS Config 呼び出します。詳細については、『Amazon VPC ユーザーガイド』の「インターフェイスエンドポイントの作成」を参照してください。

よくある質問

最新の設定変更が表示されない

設定変更をすぐに表示することは可能ですか？

AWS Config 通常、 は、変更が検出された直後、または指定した頻度でリソースの設定変更を記録します。ただし、これはベストエフォートベースであり、場合によっては時間がかかることがあります。問題がしばらく経過しても解決しない場合は、 サポートに連絡して、Amazon CloudWatch でサポートされている AWS Config メトリクスを指定します。これらの使用状況メトリクスの詳細については、「AWS Config Usage and Success Metrics」を参照してください 。

の間接的な関係 AWS Config

トピック

- リソース関係とは何ですか?
- リソースに関する直接的な関係と間接的な関係とは何ですか?
- はどの間接的な関係 AWS Config をサポートしていますか？
- 間接的な関係を使用するシナリオはどれですか？
- 直接的な関係と間接的な関係によって設定項目はどのように作成されますか?
- 間接的な関係によって生成される設定項目にはどのようなものがありますか?
- 間接的な関係を無効にするにはどうすればよいですか？
- 間接的な関係に関連する設定データを取得する方法を教えてください。

リソース関係とは何ですか?

では AWS、リソースとは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、AWS CloudFormation スタック、Amazon S3 バケットなど、管理可能なエンティティを指します。 AWS Config は、記録されたリソースタイプへの変更が検出されるたびに、または設定した記録頻度で、設定項目 (CIs) を作成してリソースを追跡およびモニタリングするサービスです。例えば、 AWS Config が Amazon EC2 インスタンスを追跡するように設定されている場合、インスタンスが作成、更新、または削除されるたびに設定項目が作成さ

れます。によって作成された各設定項目 AWS Config には、、 `arn` (Amazon リソースネーム) `accountId`、`awsRegion`、、`configurationtags`、 などの複数のフィールドがありますrelationships。CI の関係フィールドを使用すると AWS Config 、 はリソースの相互リンク方法を表示できます。例えば関係は、セキュリティグループ `sg-ef678hk` に関連付けられている Amazon EC2 インスタンス (ID は `i-a1b2c3d4`) に接続された Amazon EBS ボリューム (ID は `vol-123ab45d`) を示す場合があります。

リソースに関する直接的な関係と間接的な関係とは何ですか?

AWS Config は、ほとんどのリソースタイプの関係を「直接」関係と呼ばれる設定フィールドから取得します。直接的な関係は、リソース (A) と別のリソース (B) との間の一方向関係 (A→B) であり、通常、リソース (A) の Describe API レスポンスから取得されます。以前は、 AWS Config 最初にサポートしていた一部のリソースタイプでは、他のリソースの設定から関係もキャプチャされ、双方向 (B→A) の「間接」関係が作成されていました。例えば、Amazon EC2 インスタンスとそのセキュリティグループの関係は直接的です。セキュリティグループは Amazon EC2 インスタンスの Describe API レスポンスに含まれるためです。一方、セキュリティグループと Amazon EC2 インスタンスの関係は間接的です。セキュリティグループを記述しても、関連付けられているインスタンスに関する情報は返されないためです。

たとえば、間接的な関係は、以下の質問に答えるのに役立ちます。

- NAT ゲートウェイが失敗した場合、プライベートサブネット内のどの EC2 インスタンスが影響を受けますか？
- ルートテーブルが変更された場合、どの EC2 インスタンスで接続の問題が発生する可能性がありますか？
- 使用されたことがないセキュリティグループはどれですか？
- EC2 インスタンスにアタッチされたどのセカンダリ ENI がセキュリティグループに関連付けられていますか？

その結果、リソース設定の変更が検出されると、 はそのリソースの CI AWS Config を作成するだけでなく、間接的な関係を含む関連リソースの CIs も生成します。たとえば、 が Amazon EC2 インスタンスの変更 AWS Config を検出すると、インスタンスの CI と、インスタンスに関連付けられているセキュリティグループの CI が作成されます。

はどの間接的な関係 AWS Config をサポートしていますか？

では、次の間接的なリソース関係がサポートされています AWS Config。

リソースタイプ	は、リソースタイプに間接的に関連しています		
AWS::EC2::RouteTable	AWS::EC2::Instance , AWS::EC2::NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway , AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		

リソースタイプ	は、リソースタイプに間接的に関連しています		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

間接的な関係を使用するシナリオはどれですか？

以下は、間接的な関係を使用する AWS サービスとサービスの機能です。

AWS 機能	シナリオ
AWS Config マネージドルール	ec2-security-group-attached-to-eni ルールは、デフォルト以外のセキュリティグループが Elastic Network Interfaces (ENI) にアタッチされているかどうかを確認します。 間接的な関係がなければ、デフォルト以外のセキュリティグループが ENI にアタッチされて

AWS 機能	シナリオ
	いるかどうかを確認するカスタムルールを作成する必要があります。
AWS Firewall Manager	Usage Audit Security Group ポリシーは、間接的な関係を使用して、セキュリティグループが最後に使用された日時を把握します。 間接的な関係がなければ、ルールのトリガーを避けるために、セキュリティグループを同時に構築して新しいリソースに関連付ける必要があります AWS Firewall Manager。

デフォルトリソース	• デフォルト以外の VPC が作成された場合のデフォルトリソース：
	  • デフォルトのセキュリティグループ、デフォルトのネットワーク ACL、およびデフォルトのルートテーブル。
	• デフォルト VPC の作成時のデフォルトリソース：
	  • アクセス可能な各アベイラビリティーゾーンのデフォルト以外の VPC、インターネットゲートウェイ、デフォルトサブネットで作成されるすべての 。
	• アカウントが EC2 を初めて呼び出すときのデフォルトの VPC 作成自体。
	  • 新しく起動されたアベイラビリティーゾーンのアカウント用に作成されたデフォルトのサブネット。
	
	間接的な関係がなければ、アンチエントロピーがデフォルトリソースの変更を記録するまで最大 12 時間待つ必要があります。

直接的な関係と間接的な関係によって設定項目はどのように作成されますか？

リソース間の直接的な関係 (A→B) では、リソース B の設定を変更すると、リソース A の設定項目 (CI) も開始されます。同様に、間接的な関係 (B→A) の場合、リソース A の設定が変更されると、リソース B に新しい CI が生成されます。例えば、Amazon EC2 インスタンスとセキュリティグループは直接的な関係であるため、セキュリティグループの設定を変更すると、セキュリティグループの CI と EC2 インスタンスの CI が生成されます。同様に、セキュリティグループと Amazon EC2 インスタンスは間接的な関係であるため、EC2 インスタンスの設定を変更すると、Amazon EC2 インスタンスの CI とセキュリティグループの CI が生成されます。

間接的な関係によって生成される設定項目にはどのようなものがありますか？

以下は、間接的なリソース関係によって生成される追加の設定項目 (CI) です。

次のリソースタイプへの設定変更	は、次のリソースタイプの CI を生成します		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface` , `AWS::EC2::Subnet` , `AWS::EC2::VPNGateway` , および `AWS::EC2::VPC`		
`AWS::EC2::EIP`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface`		

次のリソースタイプへの設定変更	は、次のリソースタイプの CI を生成します		
AWS::EC2::Instance	AWS::EC2::Security Group , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::Security Group , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::Customer Gateway		
AWS::EC2::Internet Gateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

間接的な関係を無効にするにはどうすればよいですか？

間接関係を無効にするには、次の手順を実行します。

1. アカウントまたは複数のアカウントの管理アカウントから AWS サポート ケースを開きます。
2. サポートタイプのテクニカルを選択します。
3. サービス で、 を選択しますAWS Config。
4. カテゴリ で、その他 を選択します。
5. 適切な重要度レベルを選択します。
6. 件名に「間接関係を無効にする」と入力します。
7. 説明：
   - このよくある質問を読み、続行することを確認します。
   - 間接的な関係を無効にするリージョンを一覧表示します。
   - 管理アカウントから送信する場合は、アカウント IDsと関連するリージョンを含めます。
   - 複数のアカウントの場合、アカウント IDsとリージョンを含む CSV ファイルをアタッチできます。

AWS サポート エンジニアが次のステップとステータスの更新を提供します。間接的な関係が無効になっている AWS アカウントとリージョンのリストを維持することをお勧めします。新しいアカウントの場合は、間接的な関係を無効にする新しい AWS サポート ケースを送信します。

間接的な関係に関連する設定データを取得する方法を教えてください。

AWS Config 高度なクエリで構造化クエリ言語 (SQL) クエリを実行して、間接的なリソース関係に関連する設定データを取得できます。例えば、セキュリティグループに関連する Amazon EC2 インスタンスのリストを取得する場合は、次のクエリを使用します。

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

AWS SDKs AWS Config を使用するためのコード例

次のコード例は、 AWS Software Development Kit (SDK) AWS Config で を使用する方法を示しています。

アクションはより大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。アクションは個々のサービス機能を呼び出す方法を示していますが、コンテキスト内のアクションは、関連するシナリオで確認できます。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

コードの例

- AWS SDKs AWS Config を使用するための基本的な例
  - AWS SDKs AWS Config を使用するためのアクション
    - AWS SDK または CLI DeleteConfigRuleで を使用する
    - CLI で DescribeComplianceByConfigRule を使用する
    - CLI で DescribeComplianceByResource を使用する
    - CLI で DescribeConfigRuleEvaluationStatus を使用する
    - AWS SDK または CLI DescribeConfigRulesで を使用する
    - CLI で DescribeConfigurationRecorderStatus を使用する
    - CLI で DescribeConfigurationRecorders を使用する
    - CLI で DescribeDeliveryChannels を使用する
    - CLI で GetComplianceDetailsByConfigRule を使用する
    - CLI で GetComplianceDetailsByResource を使用する
    - CLI で GetComplianceSummaryByConfigRule を使用する
    - CLI で GetComplianceSummaryByResourceType を使用する
    - AWS SDK または CLI PutConfigRuleで を使用する
    - CLI で PutDeliveryChannel を使用する

AWS SDKs AWS Config を使用するための基本的な例

次のコード例は、 SDKs AWS Config で AWS の基本を使用する方法を示しています。

例

- AWS SDKs AWS Config を使用するためのアクション
  - AWS SDK または CLI DeleteConfigRuleで を使用する
  - CLI で DescribeComplianceByConfigRule を使用する
  - CLI で DescribeComplianceByResource を使用する
  - CLI で DescribeConfigRuleEvaluationStatus を使用する
  - AWS SDK または CLI DescribeConfigRulesで を使用する
  - CLI で DescribeConfigurationRecorderStatus を使用する
  - CLI で DescribeConfigurationRecorders を使用する
  - CLI で DescribeDeliveryChannels を使用する
  - CLI で GetComplianceDetailsByConfigRule を使用する
  - CLI で GetComplianceDetailsByResource を使用する
  - CLI で GetComplianceSummaryByConfigRule を使用する
  - CLI で GetComplianceSummaryByResourceType を使用する
  - AWS SDK または CLI PutConfigRuleで を使用する
  - CLI で PutDeliveryChannel を使用する

AWS SDKs AWS Config を使用するためのアクション

次のコード例は、 AWS SDKs で個々の AWS Config アクションを実行する方法を示しています。それぞれの例には、GitHub へのリンクがあり、そこにはコードの設定と実行に関する説明が記載されています。

以下の例には、最も一般的に使用されるアクションのみ含まれています。詳細な一覧については、「AWS Config API リファレンス」を参照してください。

例

- AWS SDK または CLI DeleteConfigRuleで を使用する
- CLI で DescribeComplianceByConfigRule を使用する
- CLI で DescribeComplianceByResource を使用する
- CLI で DescribeConfigRuleEvaluationStatus を使用する
- AWS SDK または CLI DescribeConfigRulesで を使用する
- CLI で DescribeConfigurationRecorderStatus を使用する

- CLI で DescribeConfigurationRecorders を使用する
- CLI で DescribeDeliveryChannels を使用する
- CLI で GetComplianceDetailsByConfigRule を使用する
- CLI で GetComplianceDetailsByResource を使用する
- CLI で GetComplianceSummaryByConfigRule を使用する
- CLI で GetComplianceSummaryByResourceType を使用する
- AWS SDK または CLI PutConfigRuleで を使用する
- CLI で PutDeliveryChannel を使用する

AWS SDK または CLI **DeleteConfigRule**で を使用する

次のサンプルコードは、`DeleteConfigRule` を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールを削除するには

次のコマンドは、 という名前 AWS の Config ルールを削除します`MyConfigRule`。

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- API の詳細については、AWS CLI コマンドリファレンスの「DeleteConfigRule」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class ConfigWrapper:
```

```
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API Reference」(AWS SDK for Python (Boto3) API リファレンス) の「DeleteConfigRule」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeComplianceByConfigRule** を使用する

次のサンプルコードは、DescribeComplianceByConfigRule を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールのコンプライアンス情報を取得するには

次のコマンドは、1 つ以上の AWS リソースによって違反された各 AWS Config ルールのコンプライアンス情報を返します。

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

出力では、各 `CappedCount` 属性の値は、関連するルールに準拠していないリソースの数を示します。例えば、次の出力は、3 つのリソースが `InstanceTypesAreT2micro` という名前のルールに準拠していないことを示しています。

出力:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeComplianceByConfigRule」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ルールの現在の評価結果がないため、INSUFFICIENT_DATA が返されるルール ebs-optimized-instance のコンプライアンスの詳細を取得します。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

出力:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

例 2: この例では、ルール ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK の非準拠リソースの数を返します。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

出力:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- API の詳細については、「 コマンドレットリファレンス (V4)」のDescribeComplianceByConfigRule」を参照してください。 AWS Tools for PowerShell

Tools for PowerShell V5

例 1: この例では、ルールの現在の評価結果がないため、INSUFFICIENT_DATA が返されるルール ebs-optimized-instance のコンプライアンスの詳細を取得します。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

出力:

```
ComplianceContributorCount ComplianceType
------------------------- --------------
                           INSUFFICIENT_DATA
```

例 2: この例では、ルール ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK の非準拠リソースの数を返します。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

出力:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のDescribeComplianceByConfigRule」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeComplianceByResource** を使用する

次のサンプルコードは、DescribeComplianceByResource を使用する方法を説明しています。

CLI

AWS CLI

AWS リソースのコンプライアンス情報を取得するには

次のコマンドは、Config によって記録され、1 つ以上のルールに違反する各 EC2 AWS インスタンスのコンプライアンス情報を返します。

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

出力では、各 CappedCount 属性の値は、リソースが違反するルールの数を示します。例えば、次の出力は、インスタンス i-1a2b3c4d が 2 つのルールに違反していることを示しています。

出力:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeComplianceByResource」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、「COMPLIANT」コンプライアンスタイプの **AWS::SSM::ManagedInstanceInventory** リソースタイプをチェックします。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

出力:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- API の詳細については、「 コマンドレットリファレンス (V4)」の DescribeComplianceByResource」を参照してください。 AWS Tools for PowerShell

Tools for PowerShell V5

例 1: この例では、「COMPLIANT」コンプライアンスタイプの **AWS::SSM::ManagedInstanceInventory** リソースタイプをチェックします。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

出力:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- API の詳細については、「 コマンドレットリファレンス (V5)」の DescribeComplianceByResource」を参照してください。 AWS Tools for PowerShell

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeConfigRuleEvaluationStatus** を使用する

次のサンプルコードは、DescribeConfigRuleEvaluationStatus を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールのステータス情報を取得するには

次のコマンドは、 という名前の AWS Config ルールのステータス情報を返しますMyConfigRule。

```
aws configservice describe-config-rule-evaluation-status --config-rule-
names MyConfigRule
```

出力:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeConfigRuleEvaluationStatus」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: このサンプルは、指定された設定ルールのステータス情報を返します。

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

出力:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V4)」の DescribeConfigRuleEvaluationStatus」を参照してください。

Tools for PowerShell V5

例 1: このサンプルは、指定された設定ルールのステータス情報を返します。

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

出力:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のDescribeConfigRuleEvaluationStatus」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DescribeConfigRules**で を使用する

次のサンプルコードは、`DescribeConfigRules` を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールの詳細を取得するには

次のコマンドは、 という名前 AWS の Config ルールの詳細を返します`InstanceTypesAreT2micro`。

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

出力:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
```

```
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeConfigRules」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: このサンプルは、選択したプロパティを持つアカウントの設定ルールを一覧表示します。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

出力:

```
ConfigRuleName                                   ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                   ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                            config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                              config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required       config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V4)」のDescribeConfigRules」を参照してください。

Tools for PowerShell V5

例 1: このサンプルは、選択したプロパティを持つアカウントの設定ルールを一覧表示します。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

出力:

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                  ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                           config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                             config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required      config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V5)」のDescribeConfigRules」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
```

```
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- API の詳細については、「AWS SDK for Python (Boto3) API Reference」(AWS SDK for Python (Boto3) API リファレンス) の「DescribeConfigRules」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeConfigurationRecorderStatus** を使用する

次のサンプルコードは、DescribeConfigurationRecorderStatus を使用する方法を説明しています。

CLI

AWS CLI

設定レコーダーのステータス情報を取得するには

次のコマンドは、デフォルトの設定レコーダーのステータスを返します。

```
aws configservice describe-configuration-recorder-status
```

出力:

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeConfigurationRecorderStatus」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: このサンプルは、設定レコーダーのステータスを返します。

```
Get-CFGConfigurationRecorderStatus
```

出力:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
```

```
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V4)」のDescribeConfigurationRecorderStatus」を参照してください。

Tools for PowerShell V5

例 1: このサンプルは、設定レコーダーのステータスを返します。

```
Get-CFGConfigurationRecorderStatus
```

出力:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V5)」のDescribeConfigurationRecorderStatus」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeConfigurationRecorders** を使用する

次のサンプルコードは、DescribeConfigurationRecorders を使用する方法を説明しています。

CLI

AWS CLI

設定レコーダーの詳細を取得するには

次のコマンドは、デフォルト設定レコーダーの詳細を返します。

```
aws configservice describe-configuration-recorders
```

出力:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeConfigurationRecorders」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、設定レコーダーの詳細を返します。

```
Get-CFGConfigurationRecorder | Format-List
```

出力:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V4)」のDescribeConfigurationRecorders」を参照してください。

Tools for PowerShell V5

例 1: この例では、設定レコーダーの詳細を返します。

```
Get-CFGConfigurationRecorder | Format-List
```

出力:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のDescribeConfigurationRecorders」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeDeliveryChannels** を使用する

次のサンプルコードは、DescribeDeliveryChannels を使用する方法を説明しています。

CLI

AWS CLI

配信チャネルの詳細を取得するには

次のコマンドは、配信チャネルに関する詳細を返します。

```
aws configservice describe-delivery-channels
```

出力:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
```

```
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeDeliveryChannels」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、リージョンの配信チャネルを取得し、詳細を表示します。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

出力:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V4)」のDescribeDeliveryChannels」を参照してください。

Tools for PowerShell V5

例 1: この例では、リージョンの配信チャネルを取得し、詳細を表示します。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

出力:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のDescribeDeliveryChannels」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetComplianceDetailsByConfigRule** を使用する

次のサンプルコードは、GetComplianceDetailsByConfigRule を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールの評価結果を取得するには

次のコマンドは、 という名前の Config AWS ルールに準拠していないすべてのリソースの評価結果を返しますInstanceTypesAreT2micro。

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

出力:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetComplianceDetailsByConfigRule」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ルール access-keys-rotated の評価結果を取得し、コンプライアンスタイプ別にグループ化された出力を返します。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

出力:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

例 2: この例では、COMPLIANT リソースの access-keys-rotated ルールのコンプライアンスの詳細をクエリします。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

出力:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V4)」の[GetComplianceDetailsByConfigRule](#)」を参照してください。

Tools for PowerShell V5

例 1: この例では、ルール access-keys-rotated の評価結果を取得し、コンプライアンスタイプ別にグループ化された出力を返します。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

出力:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
```

```
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

例 2: この例では、COMPLIANT リソースの access-keys-rotated ルールのコンプライアンスの詳細をクエリします。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

出力:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のGetComplianceDetailsByConfigRule」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetComplianceDetailsByResource** を使用する

次のサンプルコードは、`GetComplianceDetailsByResource` を使用する方法を説明しています。

CLI

AWS CLI

AWS リソースの評価結果を取得するには

次のコマンドは、EC2 インスタンス `i-1a2b3c4d` が準拠していない各ルールの評価結果を返します。

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

出力:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetComplianceDetailsByResource」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、指定されたリソースについて次のような結果が出ました。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

出力:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V4)」の GetComplianceDetailsByResource」を参照してください。

Tools for PowerShell V5

例 1: この例では、指定されたリソースについて次のような結果が出ました。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

出力:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- API の詳細については、AWS Tools for PowerShell 「コマンドレットリファレンス (V5)」の GetComplianceDetailsByResource」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetComplianceSummaryByConfigRule** を使用する

次のサンプルコードは、GetComplianceSummaryByConfigRule を使用する方法を説明しています。

CLI

AWS CLI

Config AWS ルールのコンプライアンス概要を取得するには

次のコマンドは、準拠しているルールの数と準拠していないルールの数を返します。

```
aws configservice get-compliance-summary-by-config-rule
```

出力では、各 CappedCount 属性の値は、準拠または非準拠のルールの数を示します。

出力:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetComplianceSummaryByConfigRule」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: このサンプルは、非準拠の Config ルールの数を返します。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

出力:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V4)」のGetComplianceSummaryByConfigRule」を参照してください。

Tools for PowerShell V5

例 1: このサンプルは、非準拠の Config ルールの数を返します。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

出力:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のGetComplianceSummaryByConfigRule」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetComplianceSummaryByResourceType** を使用する

次のサンプルコードは、GetComplianceSummaryByResourceType を使用する方法を説明しています。

CLI

AWS CLI

すべてのリソースタイプのコンプライアンス概要を取得するには

次のコマンドは、非準拠の AWS リソースの数と準拠しているリソースの数を返します。

```
aws configservice get-compliance-summary-by-resource-type
```

出力では、各 CappedCount 属性の値は、準拠または非準拠のリソースの数を示します。

出力:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

特定のリソースタイプのコンプライアンス概要を取得するには

次のコマンドは、準拠していない EC2 インスタンスの数と準拠しているインスタンスの数を返します。

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

出力では、各 CappedCount 属性の値は、準拠または非準拠のリソースの数を示します。

出力:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetComplianceSummaryByResourceType」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: このサンプルは、準拠または非準拠のリソースの数を返し、出力を json に変換します。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
```

```
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- API の詳細については、「 コマンドレットリファレンス (V4)」のGetComplianceSummaryByResourceType」を参照してください。 AWS Tools for PowerShell

Tools for PowerShell V5

例 1: このサンプルは、準拠または非準拠のリソースの数を返し、出力を json に変換します。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- API の詳細については、「 コマンドレットリファレンス (V5)」のGetComplianceSummaryByResourceType」を参照してください。 AWS Tools for PowerShell

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **PutConfigRule**で を使用する

次のサンプルコードは、PutConfigRule を使用する方法を説明しています。

CLI

AWS CLI

AWS マネージド Config ルールを追加するには

次のコマンドは、 AWS マネージド Config ルールを追加するための JSON コードを提供します。

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

RequiredTagsForEC2Instances.json は、ルール設定を含む JSON ファイルです。

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

ComplianceResourceTypes 属性の場合、この JSON コードはスコープを AWS::EC2::Instanceタイプのリソースに制限するため、Config AWS はルールに対して EC2 インスタンスのみを評価します。このルールはマネージドルールであるため、Owner 属性は AWS に設定され、SourceIdentifier 属性はルール識別子 REQUIRED_TAGS に設定されます。InputParameters 属性には、ルールに必要なタグキー、および CostCenter と Owner が指定されます。

コマンドが成功すると、 AWS Config は出力を返しません。ルール設定を確認するには、describe-config-rules コマンドを実行してルール名を指定します。

カスタマーマネージド Config ルールを追加するには

次のコマンドは、カスタマーマネージド Config ルールを追加するための JSON コードを提供します。

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` は、ルール設定を含む JSON ファイルです。

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

`ComplianceResourceTypes` 属性の場合、この JSON コードはスコープを `AWS::EC2::Instance`タイプのリソースに制限するため、Config AWS はルールに対して EC2 インスタンスのみを評価します。このルールはカスタマーマネージドルールであるため、 `Owner` 属性は に設定され`CUSTOM_LAMBDA`、 `SourceIdentifier` 属性は AWS Lambda 関数の ARN に設定されます。`SourceDetails` オブジェクトは必須です。`InputParameters` 属性に指定されたパラメータは、Config が呼び出してルールに対してリソースを評価するときに AWS Lambda AWS 関数に渡されます。

コマンドが成功すると、 AWS Config は出力を返しません。ルール設定を確認するには、describe-config-rules コマンドを実行してルール名を指定します。

- API の詳細については、「AWS CLI コマンドリファレンス」の「PutConfigRule」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
```

```
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API Reference」(AWS SDK for Python (Boto3) API リファレンス) の「PutConfigRule」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **PutDeliveryChannel** を使用する

次のサンプルコードは、PutDeliveryChannel を使用する方法を説明しています。

CLI

AWS CLI

配信チャネルを作成するには

次のコマンドは、配信チャネルの設定を JSON コードとして提供します。

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

deliveryChannel.json ファイルは、配信チャネルの属性を指定します。

```
{
```

```
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

この例では以下の属性を設定します。

name - 配信チャネルの名前です。デフォルトでは、 AWS Config は新しい配信チャネルdefaultに名前を割り当てます。 put-delivery-channel コマンドを使用して配信チャネル名を更新することはできません。名前を変更する手順については、「配信チャネルの名前変更」を参照してください。s3BucketName- Config が設定スナップショットと設定履歴ファイルを配信する Amazon S3 AWS バケットの名前。別の AWS アカウントに属するバケットを指定する場合、そのバケットには Config AWS にアクセス許可を付与するポリシーが必要です。詳細については、Amazon S3 バケットのアクセス許可を参照してください。

snsTopicARN - Config が設定変更に関する通知を送信する Amazon SNS トピックの Amazon リソースネーム (ARN)。別のアカウントからトピックを選択した場合、トピックには Config AWS にアクセス許可を付与するポリシーが必要です。 AWS 詳細については、「Permissions for the Amazon SNS Topic」を参照してください。

configSnapshotDeliveryProperties - Config が設定スナップショットを配信する頻度と、定期的な AWS Config ルールの評価を呼び出す頻度を設定する deliveryFrequency 属性が含まれます。

コマンドが成功すると、 AWS Config は出力を返しません。配信チャネルの設定を確認するには、describe-delivery-channels コマンドを実行します。

- API の詳細については、「AWS CLI コマンドリファレンス」の「PutDeliveryChannel」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、既存の配信チャネルの deliveryFrequency プロパティを変更します。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- API の詳細については、「 コマンドレットリファレンス (V4)」のPutDeliveryChannel」を参照してください。 AWS Tools for PowerShell

Tools for PowerShell V5

例 1: この例では、既存の配信チャネルの deliveryFrequency プロパティを変更します。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス (V5)」のPutDeliveryChannel」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Config での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

ドキュメント履歴

次の表に、 ドキュメントの重要な変更点を示します AWS Config。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

- API バージョン: 2014-11-12
- ドキュメントの最終更新日: 2025 年 7 月 15 日

変更	説明	日付
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい AWS Backup、 AWS Billing and Cost Management、 AWS CloudFormation Amazon CloudFront、 AWS Entity Resolution AWS IoT、AWS Private Certificate Authority、Amazon Relational Database Service、Amazon S3 リソースタイプの設定変更を記録できます。詳細については、「サポートされているリソースタイプ」を参照してください。	2025 年 7 月 15 日
セキュリティ IAM 更新	`AWS_ConfigRole` ポリシーと `AWSConfigServiceRolePolicy` ポリシーは AWS Backup gateway、、Amazon Bedrock AWS Billing and Cost Management、、 AWS CloudFormation Amazon CloudFront、 AWS Entity Resolution、 AWS IoT Core Device	2025 年 6 月 18 日

	Advisor AWS Lambda、 AWS Network Manager、 AWS Private Certificate Authority 、Amazon Redshift、Amazon S3 Tables、 に対する追加のアクセス許可を付与するようになりました AWS Systems Manager Quick Setup。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して新しい Amazon Bedrock リソースタイプの設定変更を記録できます。詳細については、「サポートされているリソースタイプ」を参照してください。	2025 年 6 月 17 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • cloudfront-ssl-policy-check • cognito-identity-pool-unauth-access-check • ec2-enis-source-destination-check-enabled • elbv2-listener-encryption-in-transit • lambda-function-xray-enabled • msk-cluster-public-access-disabled • msk-connect-connector-logging-enabled • msk-unrestricted-access-check • aurora-mysql-cluster-audit-logging • redshift-cluster-multi-az-enabled • s3express-dir-bucket-lifecycle-rules-check • ssm-automation-logging-enabled • ssm-automation-block-public-sharing	2025 年 6 月 13 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon Bedrock に追加のアクセス許可を付与するようになりました。詳細については、「AWS ConfigのAWSマネージドポリシー」を参照してください。	2025 年 5 月 27 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon App Integrations、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Inspector、Amazon Macie、Amazon Route 53 Profiles、Amazon OpenSearch Serverless、Amazon Simple Storage Service (Amazon S3) AWS Security Hub、Amazon SageMaker AI リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2025 年 4 月 30 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートします: redshift-serverless-default-db-name-check	2025 年 4 月 22 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートします: redshift-serverless-default-admin-check	2025 年 4 月 17 日
セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは AWS B2B Data Interchange、、Amazon Bedrock、AWS Clean Rooms、 AWS CodeConnections AWS Direct Connect、 AWS Database Migration Service（AWS DMS）、Amazon CloudWatch Logs、Amazon Macie、Amazon Managed Blockchain、Amazon Q Business、Route 53 Profiles、Amazon Simple Storage Service (Amazon S3)、Amazon SageMaker AI、 AWS Security Hub、 AWS Systems Manager Incident Manager、AWS Systems Manager Incident Manager Contacts、および に追加のアクセス許可を付与するようになりました AWS Systems Manager。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2025 年 4 月 8 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • s3-bucket-tagged • ecr-repository-tagged • sagemaker-feature-group-tagged • sagemaker-domain-tagged • cognito-user-pool-tagged	2025 年 4 月 1 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • nlb-cross-zone-load-balancing-enabled • redshift-serverless-publish-logs-to-cloudwatch • rds-instance-subnet-igw-check • ec2-spot-fleet-request-ct-encryption-at-rest • redshift-serverless-workgroup-encrypted-in-transit • redshift-serverless-workgroup-no-public-access • redshift-serverless-namespace-cmk-encryption • event-data-store-cmk-encryption-enabled • ecs-task-definition-network-mode-not-host • rds-proxy-tls-encryption • nlb-logging-enabled • redshift-audit-logging-enabled • s3-lifecycle-policy-check • sagemaker-image-tagged • redshift-cluster-parameter-group-tagged • ec2-dhcp-options-tagged • sagemaker-app-image-config-tagged	2025 年 3 月 22 日

- mariadb-publish-logs-to-cloudwatch-logs
- docdb-cluster-encrypted-in-transit
- rds-sqlserver-encrypted-in-transit
- ec2-traffic-mirror-session-tagged
- ec2-launch-template-tagged
- ec2-traffic-mirror-target-tagged
- transfer-certificate-tagged
- batch-managed-compute-env-compute-resources-tagged
- lightsail-disk-tagged
- transfer-profile-tagged
- amplify-app-tagged
- ec2-prefix-list-tagged
- amplify-branch-tagged
- transfer-agreement-tagged
- datasync-task-tagged
- transfer-workflow-tagged
- sagemaker_notebook_instance_platform_version
- ec2-traffic-mirror-filter-tagged
- aurora-mysql-cluster-audit-logging
- ssm-document-tagged
- transfer-connector-tagged

- rds-mariadb-instance-encrypted-in-transit
- iam-saml-provider-tagged
- ec2-fleet-tagged
- iam-server-certificate-tagged
- iam-oidc-provider-tagged
- alb-listener-tagged
- glb-listener-tagged
- ec2-network-insights-access-scope-tagged
- lightsail-certificate-tagged
- ec2-capacity-reservation-tagged
- ec2-transit-gateway-multicast-domain-tagged
- dms-endpoint-tagged
- ec2-carrier-gateway-tagged
- dms-replication-task-tagged
- ec2-client-vpn-endpoint-tagged
- lightsail-バケットタグ付き
- ec2-network-insights-access-scope-analysis-tagged
- nlb-listener-tagged
- EC2-network-insights-path-tagged

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • docdb-cluster-encrypted-in-transit • mariadb-publish-logs-to-cloudwatch-logs • aurora-mysql-cluster-audit-logging • rds-mariadb-instance-encrypted-in-transit • rds-sqlserver-encrypted-in-transit • sagemaker-notebook-instance-platform-version • appstream-fleet-multi-az • apprunner-vpc-connector-multi-az • mq-broker-general-logging-enabled • mq-active-single-instance-broker-storage-type-efs • mq-active-broker-ldap-authentication • iottwinmaker-component-type-tagged	2025 年 3 月 19 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • fsx-openzfs-deployment-type-check • fsx-ontap-deployment-type-check • fsx-windows-deployment-type-check • redshift-serverless-workgroup-routes-within-vpc	2025 年 3 月 18 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートします: ec2-instance-launched-with-allowed-ami	2025 年 3 月 11 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • connect-instance-logging-enabled • ecr-repository-cmk-encryption-enabled • elbv2-predefined-security-policy-ssl-check • glue-spark-job-supported-version • guardduty-runtime-monitoring-enabled • guardduty-ecs-protection-runtime-enabled • guardduty-ec2-protection-runtime-enabled • netfw-subnet-change-protection-enabled • rds-sql-server-logs-to-cloudwatch • sqs-queue-no-public-access • transfer-connector-logging-enabled	2025 年 3 月 7 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon Elastic Compute Cloud (Amazon EC2) に追加のアクセス許可を付与するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2025 年 3 月 4 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • athena-workgroup-description • amplify-app-tagged • sagemaker-app-image-config-tagged • elasticbeanstalk-application-version-description • amplify-branch-performance-mode-enabled • athena-workgroup-engine-version-auto-upgrade • sagemaker-image-description • devicefarm-instance-profile-tagged • transfer-workflow-description • ec2-traffic-mirror-session-tagged • appstream-fleet-in-vpc • transfer-agreement-tagged • ec2-traffic-mirror-target-description • transfer-agreement-description • athena-prepared-statement-description	2025 年 2 月 8 日

- batch-managed-compute-env-compute-resources-tagged
- codedeploy-deployment-group-auto-rollback-enabled
- batch-managed-compute-environment-using-launch-template
- ec2-prefix-list-tagged
- ec2-traffic-mirror-filter-tagged
- athena-workgroup-enforce-workgroup-configuration
- transfer-certificate-tagged
- batch-compute-environment-managed
- lightsail-disk-tagged
- transfer-profile-tagged
- ec2-traffic-mirror-target-tagged
- appintegrations-event-integration-tagged
- datasync-task-tagged
- batch-compute-environment-enabled
- appconfig-configuration-profile-validators-not-empty
- elasticbeanstalk-application-description
- codedeploy-deployment-group-outdated-instances-update
- ec2-launch-template-tagged

- fis-experiment-template-tagged
- ivs-channel-playback-authorization-enabled
- redshift-cluster-parameter-group-tagged
- ec2-traffic-mirror-filter-description
- appintegrations-event-integration-description
- athena-data-catalog-description
- fis-experiment-template-log-configuration-exists
- amplify-app-description
- amplify-branch-tagged
- batch-job-queue-enabled
- elasticbeanstalk-environment-description
- amplify-app-branch-auto-deletion-enabled
- appconfig-hosted-configuration-version-description
- appconfig-freeform-profile-config-storage
- datasync-task-data-verification-enabled
- apprunner-service-observability-enabled
- transfer-certificate-description
- appconfig-deployment-strategy-replicate-to-ssm

	• transfer-workflow-tagged • transfer-connector-tagged • ec2-traffic-mirror-session-description • customerprofiles-object-type-allow-profile-creation • sagemaker-image-tagged	
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Simple Storage Service (Amazon S3) リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2025 年 2 月 6 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Simple Storage Service (Amazon S3) リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2025 年 1月 29 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは AWS Clean Rooms、、Amazon Comprehend、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Simple Storage Service (Amazon S3) AWS HealthOmics、Amazon Simple Email Service (Amazon SES) に追加のアクセス許可を付与するようになりました。Amazon S3 詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2025 年 1 月 16 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • appmesh-mesh-deny-tcp-forwarding • sagemaker-model-isolation-enabled • evidently-project-description • alb-internal-scheme-check • evidently-segment-description • appconfig-environment-description • apprunner-service-in-vpc • sagemaker-domain-in-vpc • nlb-internal-scheme-check • emr-security-configuration-encryption-rest • apprunner-service-no-public-access • sagemaker-model-in-vpc • appconfig-deployment-strategy-description • evidently-launch-description • iot-authorizer-token-signing-enabled	2025 年 1 月 9 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Elastic Compute Cloud (Amazon EC2) リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2025 年 1 月 9 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • batch-job-queue-tagged • iottwinmaker-sync-job-tagged • codeguruprofiler-profiling-group-tagged • ivs-recording-configuration-tagged • iottwinmaker-entity-tagged • iottwinmaker-workspace-tagged • iottwinmaker-scene-tagged • acmpca-certificate-authority-tagged • appflow-flow-tagged • iotevents-detector-model-tagged • appmesh-virtual-node-logging-file-path-exists • apprunner-vpc-connector-tagged • apprunner-service-tagged • iotwireless-fuota-task-tagged • appmesh-virtual-node-backend-defaults-tls-on • codegururevieweer-repository-association-tagged • iotevents-input-tagged	2025 年 1 月 8 日

- appmesh-virtual-gateway-logging-file-path-exists
- batch-compute-environment-tagged
- batch-scheduling-policy-tagged
- customerprofiles-object-type-tagged
- emr-security-configuration-encryption-transit
- iotwireless-service-profile-tagged
- ivs-playback-key-pair-tagged
- cassandra-keyspace-tagged
- iotevents-alarm-model-tagged
- appconfig-application-description
- appmesh-virtual-gateway-backend-defaults-tls
- ivs-channel-tagged
- iotwireless-multicast-group-tagged

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Cognito AWS Elemental MediaConnect、Amazon OpenSearch Service リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2024 年 12 月 19 日
セキュリティ IAM 更新	このAWSConfigServiceRolePolicy ポリシーは、 に追加のアクセス許可を付与するようになりました AWS Organizations。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2024 年 12 月 18 日

AWS Config がサービスにリンクされた設定レコーダーをサポート	このリリースでは、 はサービスにリンクされた設定レコーダー AWS Config をサポートします。サポートされているサービスまたは を使用してサービスにリンクされた設定レコーダーを有効にすると AWS CLI、レコーダーはユーザーに代わってリンクされたサービスに必要なリソースタイプを記録します。 AWS Config コンソールまたは を使用して、サービスにリンクされた設定レコーダーの詳細を表示できます AWS CLI。詳細については、「設定レコーダーの使用」を参照してください。	2024 年 11 月 27 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • appconfig-application-tagged • appconfig-configuration-profile-tagged • appconfig-environment-tagged • appconfig-extension-association-tagged • appmesh-gateway-route-tagged • appmesh-mesh-tagged • appmesh-route-tagged • appmesh-virtual-gateway-tagged • appmesh-virtual-node-tagged • appmesh-virtual-router-tagged • appmesh-virtual-service-tagged • evidently-launch-tagged • evidently-project-tagged • evidently-segment-tagged • frauddetector-entity-type-tagged • frauddetector-label-tagged • frauddetector-outcome-tagged	2024 年 11 月 12 日

- frauddetector-variable-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーとポリシーは AWS AppConfig 、、Amazon Connect AWS CloudTrail、Amazon DataZone、Amazon DevOpsGuru、 AWS Glue Identity Store AWS IoT、AWS IoT FleetWise、Amazon Interactive Video Service (Amazon IVS) AWS IoT Wireless、Amazon CloudWatch Logs、Amazon CloudWatch Observability Access Manager AWS Payment Cryptography、Amazon Relational Database Service (Amazon RDS)、Amazon Rekognition、Amazon Simple Storage Service (Amazon S3)、Amazon EventBridge Scheduler AWS Systems Manager、Amazon VPC Lattice に追加のアクセス許可を付与する`AWS_ConfigRole` ようになりました。詳細については、「AWS Configのマネージドポリシー」を参照してください。	2024 年 11 月 8 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートします。cognito-user-pool-advanced-security-enabled	2024 年 11 月 6 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • active-mq-supported-version • rabbit-mq-supported-version • ec2-vpn-connection-logging-enabled • appsync-cache-ct-encryption-at-rest • appsync-cache-ct-encryption-in-transit • vpc-endpoint-enabled • efs-filesystem-ct-encrypted • redshift-cluster-subnet-group-multi-az • sns-topic-no-public-access • rabbit-mq-supported-version • kms-key-policy-no-public-access • rds-mysql-instance-encrypted-in-transit • rds-postgres-instance-encrypted-in-transit • rds-sql-server-logs-to-cloudwatch • ec2-launch-template-imdsv2-check	2024 年 10 月 21 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • PCI DSS 4.0 の運用上のベストプラクティス (グローバルリソースタイプを除く) • PCI DSS 4.0 の運用上のベストプラクティス (グローバルリソースタイプを含む)	2024 年 9 月 23 日
セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon OpenSearch Service Severless、Amazon AppStream AWS Backup、AWS CloudTrail、 AWS Glue EC2 Image Builder、 AWS IoT Amazon Interactive Video Service (Amazon IVS) AWS Elemental MediaConnect、AWS Elemental MediaTailor AWS HealthOmics、および Amazon EventBridge スケジューラに追加のアクセス許可を付与するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2024 年 9 月 16 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • ec2-resources-in-logically-air-gapped-vault • ebs-resources-in-logically-air-gapped-vault • aurora-resources-in-logically-air-gapped-vault • efs-resources-in-logically-air-gapped-vault • s3-resources-in-logically-air-gapped-vault • storagegateway-resources-in-logically-air-gapped-vault • virtualmachine-resources-in-logically-air-gapped-vault	2024 年 9 月 3 日
AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • FedRAMP (High Part 1) の運用のベストプラクティス • FedRAMP (High Part 2) の運用のベストプラクティス	2024 年 8 月 27 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • athena-workgroup-logging-enabled • codebuild-report-group-encrypted-at-rest • cognito-user-pool-advanced-security-enabled • datasync-task-logging-enabled • efs-automatic-backups-enabled • glue-job-logging-enabled • glue-ml-transform-encrypted-at-rest • kinesis-stream-backup-retention-check • rds-aurora-postgresql-logs-to-cloudwatch • rds-postgresql-logs-to-cloudwatch • workspaces-root-volume-encryption-enabled • workspaces-user-volume-encryption-enabled	2024 年 7 月 22 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon Elastic File System (Amazon EFS)、Amazon Redshift、および AWS Systems Manager for SAPに追加のアクセス許可を付与するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2024 年 6 月 17 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • cloudtrail-s3-bucket-public-access-prohibited • cloudtrail-s3-bucket-access-logging	2024 年 5 月 8 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートします。iam-external-access-analyzer-enabled	2024 年 5 月 2 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • guardduty-malware-protection-enabled • guardduty-rds-protection-enabled • guardduty-s3-protection-enabled • inspector-lambda-standard-scan-enabled	2024 年 4 月 26 日
AWS Config Amazon CloudWatch による使用状況分析の簡素化	このリリースでは、 AWS Config データ使用量をモニタリングするための Amazon CloudWatch メトリクスには、請求可能な使用量のみが表示されます。つまり、請求対象外の使用状況は、 AWS Config と AWS Config コンソールに出力される Amazon CloudWatch メトリクスの両方に表示されなくなります。これにより、Amazon CloudWatch メトリクスを使用して AWS Config セットアップと使用状況を検証し、請求可能な使用状況を関連コストに関連付けることができます。詳細については、「AWS Config の使用状況と成功メトリクス」を参照してください。	2024 年 4 月 26 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートします。iam-server-certificate-expiration-check	2024 年 4 月 23 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • vpc-sg-port-restriction-check • cloudtrail-all-write-s3-data-event-check • cloudtrail-all-read-s3-data-event-check	2024 年 4 月 17 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • guardduty-eks-protection-audit-enabled • guardduty-eks-protection-runtime-enabled • guardduty-lambda-protection-enabled • inspector-ec2-scan-enabled • inspector-ecr-scan-enabled • inspector-lambda-code-scan-enabled • redshift-unrestricted-port-access	2024 年 4 月 16 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートします: efs-mount-target-public-accessible	2024 年 3 月 20 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • dms-neptune-iam-authorization-enabled • dms-mongo-db-authentication-enabled • dms-redis-tls-enabled • dax-tls-endpoint-encryption • eks-cluster-secrets-encrypted • kinesis-firehose-delivery-stream-encrypted • mq-cloudwatch-audit-log-enabled • mq-cloudwatch-audit-log-enabled • opensearch-primary-node-fault-tolerance • sagemaker-endpoint-config-prod-instance-count • service-catalog-shared-within-organization • transfer-family-server-no-ftp	2024 年 2 月 26 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon Managed Service for Prometheus、Amazon CloudWatch、Amazon Cognito、Amazon ElastiCache、Amazon FSx AWS Glue、、 AWS Identity and Access Management (IAM) AWS Lambda、 AWS RAM、Amazon Redshift Serverless、Amazon SageMaker AI、Amazon Simple Notification Service (Amazon SNS) に追加のアクセス許可を付与するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2024 年 2 月 22 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートします: s3-bucket-cross-region-replication-enabled	2024 年 2 月 12 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい AWS AppConfig、Amazon CloudWatch Evidently、AWS Identity and Access Management (IAM)、Amazon MemoryDB (MemoryDB)、Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon Redshift、および AWS Transfer Family リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2024 年 2 月 6 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートします。macie-auto-sensitive-data-discovery-check	2024 年 1 月 29 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon AppStream、 AWS Key Management Service （AWS KMS）、Amazon Relational Database Service (Amazon RDS)、Amazon Cognito、Amazon Elastic Compute Cloud (Amazon EC2)、EC2 Image Builder、AWS Ground Station AWS Mainframe Modernization、Amazon QuickSight、Amazon Redshift、および AWS Systems Manager リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2024 年 1 月 3 日

アカウントあたりのリージョンあたりの AWS Config ルールの最大数に対するサービス制限の引き上げ	このリリースでは、 は AWS リージョンごとにアカウントごとに 1000 AWS Config ルール AWS Config をサポートします。この引き上げは、 AWS Config マネージドルール、AWS Config カスタムルール、AWS Config コンフォーマンスパック、 AWS Security Hub コントロール、 AWS Firewall Manager ポリシー、アカウントごとのリージョンごとの AWS Backup バックアッププランなど、デプロイされたすべてのルールの合計に適用されます。詳細については、「サービス制限」を参照してください。	2023 年 12 月 19 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • s3-meets-restore-time-target • ebs-meets-restore-time-target • ec2-meets-restore-time-target • rds-meets-restore-time-target • efs-meets-restore-time-target • fsx-meets-restore-time-target • aurora-meets-restore-time-target • dynamodb-meets-restore-time-target	2023 年 12 月 19 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは AWS AppConfig 、、Amazon Managed Service for Prometheus、AWS Database Migration Service（AWS DMS）、(AWS Identity and Access Management) IAM、Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon CloudWatch Logs AWS Organizations、Amazon Simple Storage Service (Amazon S3) に追加のアクセス許可を付与するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2023 年 12 月 5 日

プレビューリリース: 高度なクエリ用の自然言語クエリプロセッサ	このリリースを使用し、生成人工知能 (生成 AI) 機能を使用する高度なクエリ用の自然言語クエリプロセッサを使用できます。これにより、平易な英語で質問し、すぐに使用できるクエリ形式に変換できます。自然言語クエリプロセッサを使用すると、 AWS アカウント または AWS 組織全体でクエリを実行できます。詳細については、「Natural language query processor for advanced queries」を参照してください。	2023 年 11 月 26 日

定期記録	このリリースでは、 は定期的な記録 AWS Config をサポートしています。一定時間のリソースに対する最新の設定変更をキャプチャする機能を使用して、定期記録を行います。設定レコーダーのデフォルトの頻度を毎日に設定できるようになりました。これにより、以前に記録された CI と異なる場合にのみ、過去 24 時間におけるリソースの最新の状態を表す設定項目 (CI) を、受け取ることができます。AWS Config コンソールには、特定のリソースタイプの記録頻度を上書きしたり、特定のリソースタイプを記録から除外したりできる新しい記録戦略エクスペリエンスも導入されています。これにより、設定をきめ細かな要件に合わせることができます。 次のデータ型が追加されました。 • RecordingMode • RecordingModeOverride 次のデータ型が更新されました。 • PutConfigurationRecorder • ConfigurationRecorder • BaseConfigurationItem	2023 年 11 月 26 日

- ConfigurationItem

デベロッパーガイドの次のページが更新されました:

- AWS リソースの復号
- AWS Config コンソール AWS Config を使用したセットアップ | ワンクリックセットアップ
- AWS Config コンソールを使用したセットアップ AWS Config | 手動セットアップ
- CLI AWS を使用した のセットアップ AWS Config

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon Cognito、Amazon Connect、Amazon EMR、 AWS Ground Station AWS Mainframe Modernization、Amazon MemoryDB、AWS Organizations Amazon QuickSight、Amazon Relational Database Service (Amazon RDS)、Amazon Redshift、Amazon Route 53 AWS Service Catalog、および に対する追加のアクセス許可を付与するようになりました AWS Transfer Family。 `AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーにより、`AWSConfigServiceRolePolicyStatementID` 、`AWSConfigSLRLogStatementID` 、`AWSConfigSLRLogEventStatementID` 、`AWSConfigSLRApiGatewayStatementID` 、および `AWSConfigServiceRolePolicy` ポリシーのセキュリティ識別子 (SID) も追加できるようになりました。	2023 年 11 月 17 日

	詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • acm-pca-root-ca-disabled • dynamodb-table-deletion-protection-enabled • ec2-client-vpn-connection-log-enabled • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-configured • fsx-openzfs-copy-tags-enabled • fsx-lustre-copy-tags-to-backups • msk-enhanced-monitoring-enabled • mq-auto-minor-version-upgrade-enabled • neptune-cluster-multi-az-enabled • opensearch-update-check • s3-access-point-in-vpc-only • s3-access-point-public-access-blocks • s3-bucket-mfa-delete-enabled	2023 年 11 月 9 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい AWS Identity and Access Management (IAM) AWS Network Manager、、 AWS Private Certificate Authority （ AWS Private CA ） AWS App Mesh、Amazon Connect、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Container Service (Amazon ECS) AWS IoT、 AWS IoT TwinMaker、Amazon Managed Streaming for Apache Kafka Connect (Amazon MSK Connect) AWS Lambda、、および AWS Resource Explorer リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 11 月 3 日
AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config を更新します: BNM RMiT の運用上のベストプラクティス	2023 年 10 月 26 日

アグリゲータ用のコンプライアンスダッシュボードとインベントリダッシュボード	このリリースでは、 はコンプライアンスダッシュボードページとインベントリダッシュボードページを AWS Config コンソールの集約ビュー AWS Config に追加します。 コンプライアンスダッシュボードページに関し、非準拠リソース別のリソースタイプ上位 10 件、非準拠ルール別のアカウントレベルの適合パック上位 10 件など、アグリゲータ内のリソースコンプライアンスに関するインサイトをまとめたウィジェットのある自動ダッシュボードを表示できます。 インベントリダッシュボードページに関し、リソース数別のリソースタイプ上位 10 件、リソース数別のアカウント上位 10 件など、アグリゲータ内のリソース設定データに関するインサイトをまとめたウィジェットのある自動ダッシュボードを表示できます。 グラフやチャートについては、「Compliance dashboard」と「Inventory dashboard」を参照してください。	2023 年 10 月 23 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーとポリシーは AWS Private CA、、AWS App Mesh、Amazon Connect、Amazon Elastic Container Service (Amazon ECS)、Amazon CloudWatch Evidently、Amazon Managed Grafana、Amazon GuardDuty、Amazon Inspector AWS IoT、 AWS IoT TwinMaker、Amazon Managed Streaming for Apache Kafka (Amazon MSK) AWS Lambda、 AWS Network Manager AWS Organizations、および Amazon SageMaker AI に追加のアクセス許可を付与する`AWS_ConfigRole` ようになりました。詳細については、「AWS Configのマネージドポリシー」を参照してください。	2023 年 10 月 4 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい AWS IoT、 AWS IoT TwinMaker、 AWS IoT Wireless、Amazon Personalize Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon SageMaker AI、、AWS CodeBuild Amazon AppStream、Amazon Inspector リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 10 月 4 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • docdb-cluster-deletion-protection-enabled • docdb-cluster-audit-logging-enabled • docdb-cluster-snapshot-public-prohibited • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-upgrade-check • dms-replication-task-target db-logging • dms-replication-task-source db-logging • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-enabled • route53-query-logging-enabled • rds-aurora-mysql-audit-logging-enabled • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-enabled	2023 年 9 月 21 日

	• wafv2-rulegroup-logging-enabled • msk-in-cluster-node-require-tls	
AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config を更新します。 • Amazon S3 に関する運用上のベストプラクティス • EC2 に関する運用上のベストプラクティス	2023 年 9 月 8 日
セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーは、AWS Systems Manager (Systems Manager) の権限が削除されるようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2023 年 9 月 6 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon CodeGuru Profiler、AWS Elemental MediaConnect、 AWS Transfer Family Amazon Managed Service for Prometheus AWS Batch、AWS Cloud Mapおよび Amazon Route 53 Resolver リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 9 月 6 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • athena-workgroup-encrypted-at-rest • neptune-cluster-iam-database-authentication • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-export-enabled • neptune-cluster-deletion-protection-enabled • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-check • neptune-cluster-encrypted • neptune-cluster-snapshot-public-prohibited • docdb-cluster-backup-retention-check • docdb-cluster-encrypted • rds-cluster-encrypted-at-rest	2023 年 8 月 10 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい AWS Amplify、Amazon AppIntegrations、 AWS App Mesh Amazon Athena、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon CloudWatch Evidently 、Amazon Forecast AWS IoT Greengrass Version 2、 AWS Ground Station、、Amazon Managed Streaming for Apache Kafka (Amazon MSK) AWS Elemental MediaConvert AWS Elemental MediaTailor、Amazon Personalize、Amazon Pinpoint、および AWS Resilience Hub リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 8 月 3 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと`AWS_ConfigRole` ポリシーは AWS App Mesh、Amazon AppStream 2.0、 AWS CloudFormation Amazon CloudFront、 AWS CodeArtifact AWS CodeBuild Amazon Connect、 AWS Glue Amazon GuardDuty、AWS Identity and Access Management (IAM)、Amazon Inspector、 AWS IoT AWS IoT TwinMaker、 AWS IoT Wireless、Amazon Managed Streaming for Apache Kafka、Amazon Macie、AWS Elemental MediaConnect AWS Network Manager AWS Organizations、 AWS Resource Explorer、Amazon Route 53、Amazon Simple Storage Service (Amazon S3)、Amazon Simple Notification Service (Amazon SNS)、および Amazon EC2 Systems Manager (SSM) の Amazon Managed Workflows に追加のアクセス許可を付与するようになりました。 Amazon EC2 Systems Manager 詳細については、「AWS ConfigのAWSマネージドポリシー」を参照してください。	2023 年 7 月 28 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Kinesis、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Pinpoint、Amazon Simple Storage Service (Amazon S3)、Amazon Virtual Private Cloud (Amazon VPC) AWS App Runner、Amazon Kendra、Amazon Connect AWS CloudFormation、AWS AppConfig AWS App Mesh、および AWS Database Migration Service (AWS DMS) リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 7 月 10 日
組織のコンフォーマンスパックのサービス制限が引き上げられる	このリリースでは、 はすべてのコンフォーマンスパックでアカウントごとにリージョンあたり 350 の AWS Config ルールをサポートし、組織ごとに 350 の組織 AWS Config ルール AWS Config をサポートします。詳細については、「 サービス制限」を参照してください。	2023 年 6 月 13 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon Managed Workflows に追加のアクセス許可を付与するようになりました AWS Amplify。 Amazon Connect、 AWS App Mesh、 Amazon Managed Service for Prometheus Amazon Athena、 AWS Batch AWS CloudFormation、 AWS CloudTrail、 AWS CodeArtifact、、 Amazon CodeGuru、 AWS Directory Service、 Amazon DynamoDB、 Amazon Elastic Compute Cloud (Amazon EC2)、 Amazon CloudWatch Evidently、 Amazon Forecast、 AWS Organizations AWS IoT Greengrass、 AWS Ground Station、 AWS Identity and Access Management（IAM)、 Amazon Managed Streaming for Apache Kafka (Amazon MSK)Amazon Lightsail、、 Amazon CloudWatch Logs、 AWS Elemental MediaConnect、 AWS Elemental MediaTailor、 Amazon Pinpoint、 Amazon Virtual Private Cloud (Amazon VPC) Amazon Personalize、 Amazon QuickSight、 AWS Migration Hub Refactor	2023 年 6 月 13 日

Spaces、 Amazon Simple Storage Service (Amazon S3) Amazon SageMaker AI、 および AWS Transfer Family。詳細については、「AWS Configのマネージドポリシー」を参照してください。

AWS Config リソースタイプ別の除外の記録	このリリース AWS Config では、 では、インベントリ追跡とコンプライアンスモニタリングから特定のタイプの AWS リソースを除外しながら、将来追加されるリソースタイプを含め AWS Config、現在利用可能な他のすべてのサポートされているリソースタイプを追跡できます。この機能を使用すると、コンプライアンスおよびガバナンスの基準が適用される重要なリソースに注力できます。 設定レコーダーと記録グループの API の更新は下位互換性があるため、以前のバージョンの PutConfigurationRecorder API でも機能します。更新された API や新しい API を使用しなくても、これまでとまったく同じ方法で、記録するリソースタイプの管理を継続できます。 次のデータ型が追加されました。 • RecordingStrategy • ExclusionByResourceTypes 次のデータ型が更新されました。 • PutConfigurationRecorder • ConfigurationRecorder	2023 年 6 月 9 日

	• RecordingGroup 開発者ガイドの次のページが更新されました。 • 記録対象のリソースの選択	
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Elastic Container Service (Amazon ECS)、Amazon Keyspaces (Apache Cassandra 用) (Amazon Keyspaces) AWS Signer、 AWS Amplify、AWS App Mesh、 AWS App Runner、Amazon AppStream 2.0、Amazon Elastic Compute Cloud (Amazon EC2) AWS CodeArtifact、Amazon CloudWatch Evidently、Amazon Forecast、AWS Identity and Access Management (IAM)、Amazon Pinpoint、Amazon SageMaker AI AWS Transfer Family、Amazon Data Firehose リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 6 月 5 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • cloudfront-s3-origin-access-control-enabled • custom-schema-registry-policy-attached • ec2-client-vpn-not-authorize-all • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-upgrade-enabled • mq-cloudwatch-audit-logging-enabled • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-logging-enabled	2023 年 5 月 10 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Route 53 Resolver、Amazon Elastic Compute Cloud (Amazon EC2)、 AWS IoT Wireless、 AWS Network Manager AWS Device Farm、AWS Ground Station、Amazon AppFlow、Amazon Redshift、Amazon Pinpoint、AWS IoT AWS AppConfig、EC2 Image Builder、Amazon CloudWatch、Amazon SageMaker Runtime AWS Panorama、Amazon ECR、および AWS Audit Manager リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 5 月 5 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して の設定変更を記録できます`AWS::NetworkFirewall::TLSInspectionConfiguration` 。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 5 月 1 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーとポリシーは AWS Amplify、、AWS App Runner、Amazon CloudFront AWS App Mesh、、 AWS CodeArtifact Amazon Elastic Compute Cloud、Amazon Kendra、Amazon Macie、Amazon Route 53、Amazon SageMaker AI、AWS Transfer Family、Amazon Pinpoint、 AWS Resilience Hub AWS Migration Hub、Amazon CloudWatch、 AWS Directory Service、および の Amazon Managed Workflows に追加のアクセス許可を付与する`AWS_ConfigRole` ようになりました AWS WAF。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2023 年 4 月 13 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • elasticache-auto-minor-version-upgrade-check • elasticache-repl-grp-auto-failover-enabled • elasticache-repl-grp-encrypted-at-rest • elasticache-repl-grp-encrypted-in-transit • elasticache-repl-grp-redis-auth-enabled • elasticache-subnet-group-check • cloudfront-s3-origin-non-existent-bucket	2023 年 4 月 10 日
組織のコンフォーマンスパックのサービス制限が引き上げられる	このリリースでは、 はすべての組織コンフォーマンスパックでアカウントあたり 350 AWS Config ルール AWS Config をサポートします。詳細については、「サービス制限」を参照してください。	2023 年 4 月 3 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-rest	2023 年 4 月 3 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon AppStream 2.0、 AWS Auto Scaling、Amazon Connect Amazon Elastic Compute Cloud、Amazon EventBridge、Health Lake、Kinesis ビデオストリーム、 AWS IoT TwinMaker 、Lookout for Vision、Network Manager、Amazon Pinpoint、Amazon Application Recovery Controller (ARC)、および AWS RoboMaker リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 4 月 3 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーとポリシーは、Amazon AppFlow AWS App Runner、、Amazon AppStream 2.0、AWS CloudFormation Amazon CloudFront、Amazon CloudWatch、 AWS CodeArtifact AWS CodeCommit AWS Device Farm、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon CloudWatch Evidently、Amazon Forecast、AWS Ground Station、AWS Identity and Access Management (IAM) AWS IoT、Amazon MemoryDB、Amazon Pinpoint、 AWS Network Manager AWS Panorama、Amazon Relational Database Service (Amazon RDS)、Amazon Redshift、Amazon SageMaker AI の Amazon Managed Workflows に追加のアクセス許可を付与する`AWS_ConfigRole` ようになりました。詳細については、「AWS Configのマネージドポリシー」を参照してください。	2023 年 3 月 30 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーでは、 AWS Audit Manager に対する追加のアクセス権限がサポートされるようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2023 年 3 月 3 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい AWS Elemental MediaPackage、Amazon EventBridge、(Amazon Simple Storage Service (Amazon S3) AWS IoT、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Lookout for Metrics、Amazon Lex、 AWS Budgets AWS Device Farm、Amazon CodeGuru Reviewer Amazon Route 53 Resolver、および AWS RoboMaker リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 3 月 2 日

セキュリティ IAM 更新	AWS Config は、`AWSConfigMultiAccountSetupPolicy` ポリシーの変更を追跡するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2023 年 2 月 27 日
AWS Config リージョンの可用性別のリソースカバレッジ	このリリースでは、 はサポートされている各リソースタイプのリージョン情報 AWS Config を提供します。どのリソースタイプがどのリージョンでサポートされているかについては、「利用可能なリージョン別リソースカバレッジ」を参照してください。	2023 年 2 月 20 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Interactive Video Service (Amazon IVS)、Amazon Simple Storage Service (Amazon S3) AWS Glue、Amazon Elastic Kubernetes Service (Amazon EKS)、Amazon Relational Database Service (Amazon RDS) AWS IoT、Managed Service for Apache Flink リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 2 月 7 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーとポリシーは、Amazon Managed Workflows for Apache Airflow、 AWS IoT Amazon AppStream 2.0、Amazon CodeGuru Reviewer、AWS HealthLake、Amazon Kinesis Video Streams、Amazon Application Recovery Controller (ARC)、Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm、Amazon Pinpoint、AWS Identity and Access Management (IAM)、Amazon GuardDuty、Amazon CloudWatch Logs に追加のアクセス許可を付与する`AWS_ConfigRole` ようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2023 年 2 月 1 日
セキュリティ IAM 更新	セキュリティのベストプラクティスとして、`ConfigConformsServiceRolePolicy` ポリシーでは `config:DescribeConfigRules` に対する広範なリソースレベルのアクセス許可を削除するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2023 年 1 月 12 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon Managed Service for Prometheus、AWS Audit Manager、 AWS Database Migration Service（AWS DMS）AWS Device Farm、 AWS Directory Service Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue、 AWS IoT、Amazon Lightsail AWS Elemental MediaPackage、、AWS Network Manager、Amazon QuickSight、Amazon Application Recovery Controller (ARC)、Amazon Simple Storage Service (Amazon S3) AWS Resource Access Manager、および Amazon Timestream に追加のアクセス許可を付与するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2023 年 1 月 10 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon MQ、 AWS AppConfig AWS Cloud9、Amazon EventBridge スキーマ、Amazon Fraud Detector、AWS IoT、 AWS IoT Analytics 、 AWS Elemental MediaPackage (MediaPackage)Amazon Lightsail、Amazon Application Recovery Controller (ARC) AWS Resilience Hub、および AWS Transfer Family リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2023 年 1 月 5 日
AWS Config ルールリソースカバレッジ	このリリースでは、 は、増加した AWS Config マネージドルールのリソースタイプカバレッジ AWS Config を表示します。	2022 年 12 月 21 日
AWS Config ルールの検出可能性	このリリースでは、 は評価モード別の AWS Config マネージドルールのリスト、トリガータイプ別の AWS Config マネージドルールのリスト、リージョンの可用性別のマネージドルールのリストの AWS Configページ AWS Config をサポートします。	2022 年 12 月 21 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config を更新します。 • K-ISMS の運用のベストプラクティス • NIST 800 171 に関する運用上のベストプラクティス • PCI DSS 3.2.1 運用のベストプラクティス • 「Esquema Nacional de Seguridad (ENS) High」に関する運用のベストプラクティス • 「Esquema Nacional de Seguridad (ENS) Medium」に関する運用のベストプラクティス • 「Esquema Nacional de Seguridad (ENS) Low」に関する運用のベストプラクティス • NZISM 運用のベストプラクティス • NIST 800-53 rev 5の運用のベストプラクティス	2022 年 12 月 19 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • api-gwv2-access-logs-enabled • api-gwv2-authorization-type-configured • cloudfront-security-policy-check • ec2-launch-template-public-ip-disabled • elastic-beanstalk-logs-to-cloudwatch • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-access-check • security-account-information-provided • storagegateway-resources-protected-by-backup-plan • wafv2-rulegroup-not-empty • wafv2-webacl-not-empty	2022 年 12 月 9 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon CloudWatch RUM、Amazon EventBridge、Amazon GuardDuty 、Amazon Simple Email Service (Amazon SES) AWS Backup AWS DataSync、および AWS Fault Injection Service （ AWS FIS) リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 12 月 9 日

AWS Config プロアクティブコンプライアンス	このリリースでは、 はリソースのプロビジョニング前に AWS Config ルールへの準拠をプロアクティブにチェックする機能 AWS Config をサポートします。これにより、リソースの作成または更新の前に、リソース構成の設定を評価できます。 AWS Config を使用して、事前プロビジョニングまたは事後プロビジョニングのいずれかでリソースに加えられた設定変更を追跡し、リソースが目的の設定と一致するかどうかを確認します。 次のデータ型が追加されました。 • GetResourceEvaluationSummary • StartResourceEvaluation • ListResourceEvaluations 次のデータ型が更新されました。 • DescribeConfigRulesFilters • GetComplianceDetailsByResource • EvaluationResultQualifier • EvaluationModeConfiguration	2022 年 11 月 28 日

デベロッパーガイドの次のページが更新されました:

- AWS Config ルールのコンポーネント
- AWS Config ルールの評価モードとトリガータイプ
- AWS Config マネージドルール
- AWS Config カスタムルール
- AWS Config ルールの管理

設定 AWS Config レコーダーの設定項目としてのドリフト検出 (CI)	このリリースでは、 は設定レコーダーへのすべての変更 AWS Config を追跡して、設定レコーダーの状態が以前の状態と異なるかドリフトしたかを示します。たとえば、AWS Config 追跡を有効にしたリソースタイプの更新がある場合、設定レコーダーを停止または開始した場合、設定レコーダーを削除またはアンインストールした場合などです。`AWS::Config::ConfigurationRecorder` リソースタイプは のシステムリソースタイプ AWS Config であり、このリソースタイプの記録は、サポートされているすべてのリージョンでデフォルトで有効になっています。`AWS::Config::ConfigurationRecorder` リソースタイプの記録は、追加料金なしでご利用いただけます。詳細については、「設定レコーダーのドリフト検出」を参照してください。	2022 年 11 月 18 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい AWS IoT Events、 AWS Cloud Map、EC2 Image Builder AWS DataSync、、Amazon Application Recovery Controller (ARC) AWS Glue、および Amazon Elastic Container Registry (Amazon ECR) リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 11 月 8 日
セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーでは、 AWS CloudFormation に対する追加のアクセス権限がサポートされるようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2022 年 11 月 7 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • Criminal Justice Information Services (CJIS) の運用のベストプラクティス • Amazon SageMaker AI のセキュリティのベストプラクティス • Amazon Elastic Container Registry のセキュリティのベストプラクティス 次のコンフォーマンスパックが更新されました: • MAS TRMGの運用のベストプラクティス • NCSC の「Cyber Assesment Framework」に関する運用上のベストプラクティス • NCSC Cloud Security Principles に関する運用上のベストプラクティス	2022 年 10 月 27 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは AWS Certificate Manager、に追加のアクセス許可を付与するようになりました。Amazon Managed Workflows for Apache Airflow AWS Amplify、 AWS AppConfig 、 Amazon Keyspaces、Amazon CloudWatch、Amazon Connect、 AWS Glue DataBrew、 Amazon Elastic Compute Cloud (Amazon EC2)、 Amazon Elastic Kubernetes Service (Amazon EKS) Amazon EventBridge、AWS Fault Injection Service、Amazon Fraud Detector、Amazon FSx、 Amazon GameLift サーバー Amazon Location Service、 AWS IoT、 Amazon Lex、Amazon Lightsail、 Amazon Pinpoint、 OpsWorks AWS Panorama、 AWS Resource Access Manager、、Amazon QuickSight、Amazon Relational Database Service (Amazon RDS) Amazon Rekognition、 AWS RoboMaker、 AWS Resource Groups、 Amazon Route 53、 Amazon Simple Storage Service (Amazon S3) AWS Cloud Map、、 および AWS	2022 年 10 月 19 日

	Security Token Service。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Simple Email Service (Amazon SES) AWS AppConfig、 AWS Cloud Map および AWS DataSync リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 10 月 6 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon GuardDuty、Amazon SageMaker AI AWS AppSync AWS Cloud Map、および AWS DataSync リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 10 月 4 日
AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は SWIFT CSP コンフォーマンスパックの運用上のベストプラクティス AWS Config を更新します。	2022 年 10 月 4 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • CMMC 2.0 Level 1 に関する運用上のベストプラクティス • CMMC 2.0 Level 2 に関する運用上のベストプラクティス 次のコンフォーマンスパックが更新されました: • Amazon API Gateway 運用のベストプラクティス • AWS Well-Architected フレームワークの信頼性の柱に関する運用上のベストプラクティス • AWS Well-Architected フレームワークのセキュリティの柱に関する運用上のベストプラクティス • CMMC Level 1 に関する運用上のベストプラクティス • CMMC Level 2 に関する運用上のベストプラクティス • CMMC Level 3 に関する運用上のベストプラクティス • CMMC Level 4 に関する運用上のベストプラクティス • CMMC Level 5 に関する運用上のベストプラクティス	2022 年 9 月 30 日

	• FFIEC に関する運用上のベストプラクティス • FedRAMP (Low) の運用のベストプラクティス • シンガポール金融管理局の「Notice 655」の運用のベストプラクティス • NBC の「TRMG」の運用のベストプラクティス • NIST 800 172 運用のベストプラクティス	
セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーでは、 AWS Glueに対する追加のアクセス権限がサポートされるようになりました。詳細については、「AWS Configのマネージドポリシー」を参照してください。	2022 年 9 月 14 日
AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は SWIFT CSP コンフォーマンスパックの運用上のベストプラクティス AWS Config をサポートしています。	2022 年 9 月 9 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon AppFlow に追加のアクセス許可を付与するようになりました。 Amazon CloudWatch、 Amazon CloudWatch RUM、 Amazon CloudWatch Synthetics、 Amazon Connect Customer Profiles、Amazon Connect Voice ID、Amazon DevOpsGuru、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon EC2 Auto Scaling、Amazon EMR、 Amazon EventBridge、 Amazon EventBridge スキーマ、Amazon FinSpace、 Amazon Fraud Detector、 Amazon GameLift サーバー Amazon Interactive Video Service (Amazon IVS) Amazon Managed Service for Apache Flink、 EC2 Image Builder、Amazon Lex、Amazon Lightsail、 Amazon Location Service、 Amazon Lookout for Equipment、 Amazon Lookout for Metrics、 Amazon Lookout for Vision、 Amazon Managed Blockchain、Amazon MQ、 Amazon Nimble StudioAmazon Pinpoint、 Amazon QuickSigh	2022 年 9 月 7 日

t、 Amazon Application Recovery Controller (ARC) Amazon Route 53 Resolver、、 Amazon Simple Storage Service (Amazon S3) Amazon SimpleDB、 Amazon Simple Email Service (Amazon SES) Amazon Timestream、 AWS AppConfig AWS AppSync、 AWS Auto Scaling、 AWS Backup、 AWS Budgets、 AWS Cost Explorer、 AWS Cloud9 AWS Directory Service、 AWS DataSync、 AWS Elemental MediaPackage、 AWS Glue AWS IoT、 AWS IoT Events、 AWS IoT Analytics AWS IoT SiteWise、 AWS IoT TwinMaker、 AWS Lake Formation AWS License Manager、 AWS Resilience Hub、 AWS Signer、 および AWS Transfer Family。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • Amazon CloudWatch に関する運用上のベストプラクティス • ドイツのクラウドコンピューティングコンプライアンスコントロールカタログ (C5) • IRS 1075 に関する運用上のベストプラクティス 次のコンフォーマンスパックが更新されました: • AWS Control Tower Detective ガードレールコンフォーマンスパック • CISA Cyber Essentials に関する運用上のベストプラクティス • SME 向け ENISA サイバーセキュリティガイドの運用上のベストプラクティス • FDA Title 21 CFR Part 11 の運用のベストプラクティス • FedRAMP(Moderate) に関する運用上のベストプラクティス • HIPAA Security の運用のベストプラクティス	2022 年 8 月 31 日

	• NIST プライバシーフレームワーク v1.0 オペレーションのベストプラクティス • NYDFS 23 の運用のベストプラクティス • RBI の「Cyber Security Framework for UCBs」に関する運用上のベストプラクティス • RBI の「MD-ITF」の運用のベストプラクティス	
の開始方法 AWS Config とカスタムコンフォーマンスパックの更新	このリリースでは、 はコンソールの使用開始 AWS Configページとセットアップ AWS Configページ AWS Config を更新し、ワンクリックセットアップと手動セットアップページを導入します。AWS Config は、コンフォーマンスパック YAML ファイルを最初から作成する方法についてのチュートリアルでカスタムコンフォーマンスパックページも更新します。	2022 年 8 月 25 日

AWS Systems Manager ドキュメント (SSM ドキュメント) とコンフォーマンスパックの統合	今回のリリースでは、SSM ドキュメントを使用してコンフォーマンスパックテンプレートを作成できます。SSM ドキュメントの詳細については、 AWS Systems Manager ユーザーガイドの「AWS Systems Manager ドキュメント」を参照してください。 次のデータ型が更新されました。 • PutConformancePack • コンフォーマンスパックの詳細 • テンプレート SSM ドキュメントの詳細 デベロッパーガイドの次のページが更新されました: • AWS Config コンソールを使用したコンフォーマンスパックのデプロイ • AWS コマンドラインインターフェイスを使用したコンフォーマンスパックのデプロイ	2022 年 8 月 24 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon Simple Email Service (Amazon SES) AWS DataSync、および に対する追加のアクセス許可を付与するようになりました AWS Cloud Map。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2022 年 8 月 22 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Athena、Amazon Detective、Amazon SageMaker AI、Amazon Route 53、 AWS Database Migration Service（AWS DMS）、（AWS KMS） AWS Glue、 AWS Key Management Service Amazon Simple Email Service (Amazon SES) リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 8 月 16 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config を更新します。 • NIST の「1800 25」に関する運用上のベストプラクティス • NIST 800 181 運用のベストプラクティス • ABS CCIG 2.0 標準ワークロードに関する運用上のベストプラクティス • ABS CCIG 2.0 マテリアルワークロードに関する運用上のベストプラクティス • ACSC の Essential 8 に関する運用上のベストプラクティス • ACSC の「ISM」に関する運用上のベストプラクティス • APRA の「CPG 234」に関する運用上のベストプラクティス • CIS AWS Foundations Benchmark v1.4 レベル 1 の運用上のベストプラクティス • CIS AWS Foundations Benchmark v1.4 レベル 2 の運用上のベストプラクティス • BNM の「RMiT」に関する運用上のベストプラクティス	2022 年 8 月 1 日

- NIST の「CSF」に関する運用上のベストプラクティス

コンフォーマンスパックのコンプライアンススコア	このリリースでは、 にコンフォーマンスパックのコンプライアンススコア AWS Config が導入され、コンフォーマンスパックのコンプライアンス状態の概要が表示されます。これは、コンフォーマンスパックのコンプライアンスレベルを特定、調査、把握するために使用できます。コンプライアンススコアは、コンフォーマンスパック内の可能なルールとリソースの組み合わせの合計数に対する、コンフォーマンスパック内のコンプライアンスルールとリソースの組み合わせの数の割合です。 次のデータ型が更新されました。 • ListConformancePackComplianceScores • ConformancePackComplianceScore デベロッパーガイドの次のページが更新されました: • AWS Config ダッシュボードの表示 • コンフォーマンスパックのダッシュボードでのコンプライアンスデータの表示	2022 年 7 月 26 日

	• コンフォーマンスパックの管理 (API)	
セキュリティ IAM 更新	`ConfigConformsServiceRolePolicy` ポリシーは、メトリクスデータポイントを Amazon CloudWatch に発行する許可を付与するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2022 年 7 月 25 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーとポリシーは、Amazon Elastic Container Service (Amazon ECS)、Amazon ElastiCache、Amazon EventBridge、Amazon FSx、Amazon Managed Service for Apache Flink、Amazon Location Service、Amazon Managed Streaming for Apache Kafka、Amazon QuickSight、Amazon Rekognition、Amazon Simple Storage Service (Amazon S3) AWS RoboMaker、Amazon Simple Email Service (Amazon SES)、 AWS Amplify、、AWS AppConfig、 AWS AppSync、 AWS Billing Conductor AWS DataSync、AWS Firewall Manager、AWS Glue、 AWS IAM Identity Center 、 (IAM Identity Center)、EC2 Image Builder、および Elastic Load Balancing に追加のアクセス許可を付与する`AWS_ConfigRole` ようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2022 年 7 月 15 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Elastic Compute Cloud (Amazon EC2) リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 7 月 8 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して新しい AWS Global Accelerator リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 7 月 5 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • autoscaling-launch-template • ecs-task-definition-log-configuration • ecs-awsvpc-networking-enabled	2022 年 7 月 1 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • カナダサイバーセキュリティセンター (CCCS) 中規模クラウド制御プロファイルに関する運用面のベストプラクティス • グラムリーチブライリー法 (GLBA) に関する運用上のベストプラクティス • GxP EU Annex 11 に関する運用上のベストプラクティス • Amazon Elastic Kubernetes Service (Amazon EKS) でのセキュリティに関するベストプラクティス • Amazon Relational Database Service (Amazon RDS) でのセキュリティに関するベストプラクティス • のセキュリティのベストプラクティス AWS Lambda 次のコンフォーマンスパックが更新されました: • AI と機械学習に関する運用面のベストプラクティス • Amazon DynamoDB での運用面のベストプラクティス	2022 年 6 月 30 日

	• CIS の「Critical Security Controls v8 IG1」に関する運用上のベストプラクティス • CIS の「Critical Security Controls v8 IG2」に関する運用上のベストプラクティス • CIS の「Critical Security Controls v8 IG3」に関する運用上のベストプラクティス • HIPAA Security の運用のベストプラクティス • NIST 800-53 rev 5の運用のベストプラクティス • NIST の「CSF」に関する運用上のベストプラクティス	
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して新しい Amazon SageMaker AI リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 1 月 29 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon Route 53、Amazon WorkSpaces、(IAM Access Analyzer) AWS Batch、 AWS Identity and Access Management Access Analyzer AWS Database Migration Service（AWS DMS）AWS Step Functions、および Elastic Load Balancing リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 6 月 14 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • aurora-last-backup-recovery-point-created • dynamodb-last-backup-recovery-point-created • ebs-last-backup-recovery-point-created • ec2-last-backup-recovery-point-created • efs-last-backup-recovery-point-created • fsx-last-backup-recovery-point-created • rds-last-backup-recovery-point-created • s3-last-backup-recovery-point-created • storagegateway-last-backup-recovery-point-created • virtualmachine-last-backup-recovery-point-created	2022 年 6 月 13 日

AWS Config との統合 AWS Security Hub	このリリースでは、 AWS Config マネージドルールとカスタムルールの評価の結果を調査結果として確認できます AWS Security Hub。Security Hub は、ルール評価を結果に変換し、Amazon リソースネーム (ARN) や作成日など、影響を受けるリソースに関する詳細情報を提供します。これらの結果は、他の Security Hub の結果と一緒に表示でき、セキュリティ体制を包括的に概観できます。詳細については、「ルール評価を Security Hub に送信する」を参照してください。	2022 年 6 月 7 日
セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Amazon Athena、Amazon Detective、Amazon GuardDuty、Amazon Macie、Amazon Simple Email Service (Amazon SES) AWS Glue、、 AWS Resource Access Manager（AWS RAM）、および に対する追加のアクセス許可を付与するようになりました AWS IAM Identity Center。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2022 年 5 月 31 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • Amazon Elastic Container Service (Amazon ECS) のセキュリティのベストプラクティス • Amazon Elastic File System (Amazon EFS) のセキュリティのベストプラクティス • Amazon CloudFront のセキュリティのベストプラクティス • のセキュリティのベストプラクティス AWS Auto Scaling • のセキュリティのベストプラクティス AWS Network Firewall • のセキュリティのベストプラクティス AWS Secrets Manager	2022 年 5 月 31 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon SageMaker AI と AWS Step Functions リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 5 月 26 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は NERC CIP BCSI コンフォーマンスパックの運用上のベストプラクティス AWS Config を更新します。	2022 年 5 月 20 日
AWS Config ルールのコンポーネント	このリリースでは、 は ルールページのコンポーネント AWS Config AWS Config を紹介します。このページでは、ルール定義、ルールメタデータ、および Rules Development Kit (RDK) と AWS Config Rules Development Kit Library (RDKlib) を使用して Python で AWS Config ルールを作成する方法のベストプラクティスについて説明します。	2022 年 5 月 9 日
組織のコンフォーマンスパックのサービス制限が引き上げられる	このリリースでは、 はすべての組織コンフォーマンスパックでアカウントあたり 180 AWS Config ルール AWS Config をサポートします。詳細については、「サービス制限」を参照してください。	2022 年 5 月 6 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • Amazon OpenSearch Service のセキュリティベストプラクティス • Amazon Redshift のセキュリティベストプラクティス • のセキュリティのベストプラクティス AWS CloudTrail • のセキュリティのベストプラクティス AWS CodeBuild • のセキュリティのベストプラクティス AWS WAF	2022 年 4 月 29 日
AWS Config マネージドルールの更新	このリリースでは、 は s3-resources-protected-by-backup-plan マネージドルール AWS Config をサポートします。	2022 年 4 月 11 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーとポリシーは、すべてまたは指定された AWS CloudTrail イベントデータストア (EDS) に関する情報の取得、すべてまたは指定された AWS CloudFormation リソースに関する情報の取得、DynamoDB Accelerator (DAX) パラメータグループまたはサブネットグループのリストの取得、アクセス中の現在のリージョンのアカウントの AWS Database Migration Service（AWS DMS) レプリケーションタスクに関する情報の取得、および AWS Organizations 指定されたタイプの のすべてのポリシーのリストの取得を行うための追加のアクセス許可を付与する `AWS_ConfigRole` ようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2022 年 4 月 7 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-limit • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-version • netfw-policy-default-action-fragment-packets • netfw-policy-default-action-full-packets • netfw-policy-rule-group-associated • redshift-audit-logging-enabled • s3-lifecycle-policy-check • waf-regional-rule-not-empty • waf-regional-rulegroup-not-empty • waf-regional-webacl-not-empty	2022 年 4 月 4 日

	• vpc-peering-dns-resolution-check	
AWS Config カスタムポリシールール	このリリースでは、 AWS Config で AWS CloudFormation Guard (guard) を使用して AWS Config カスタムポリシールールを作成できます。Guard は、policy-as-codeポリシー言語です。 AWS Config Guard ポリシーを使用して記述されたルールは、 AWS Config コンソールまたは AWS Config ルール APIs を使用して作成できます。 デベロッパーガイドの次のページが更新されました: • AWS Config カスタムルール • Guard を使用した AWS Config カスタムルールの作成 次のデータ型が更新されました。 • ソース • CustomPolicyDetails • ConfigRuleEvaluationStatus • GetCustomRulePolicy • GetOrganizationCustomRulePolicy • OrganizationCustomPolicyRuleMetadata	2022 年 4 月 4 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon EMR SecurityConfiguration リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 3 月 31 日
AWS Config マネージドルールの更新	このリリースでは、 は virtualmachine-resources-protected-by-backup-plan マネージドルール AWS Config をサポートします。	2022 年 3 月 29 日

AWS Config Amazon CloudWatch メトリクスとの統合	このリリースでは、 は AWS Config Dashboard ページの Amazon CloudWatch で AWS Config 使用状況と成功のメトリクスの追跡をサポートする AWS Config ようになりました。CloudWatch メトリクスは、 AWS リソースに関するメトリクスでアラームを検索、グラフ化、構築する機能など、システムのパフォーマンスに関するデータを提供するモニタリングサービスです。 AWS Config ダッシュボードから、ワークフローで発生した障害の AWS Config 使用状況と主要なメトリクスの原因となっているトラフィックを確認できます。 次のページが更新されます。 • AWS Config ダッシュボードの表示	2022 年 3 月 29 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon GuardDuty Detector リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 3 月 24 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • clb-multiple-az • cloudfront-no-deprecated-ssl-protocols • cloudfront-traffic-to-origin-encrypted • cloudwatch-alarm-action-enabled-check • ec2-no-amazon-key-pair • ec2-paravirtual-instance-check • ec2-token-hop-limit-check • ec2-transit-gateway-auto-vpc-attach-disabled • ecr-private-lifecycle-policy-configured • efs-access-point-enforce-root-directory • efs-access-point-enforce-user-identity • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-check • s3-event-notifications-enabled • sns-topic-message-delivery-notification-enabled • waf-global-rulegroup-not-empty	2022 年 3 月 23 日

- waf-global-rule-not-empty

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config を更新します。 • CIS の「Critical Security Controls v8 IG1」に関する運用上のベストプラクティス • CIS の「Critical Security Controls v8 IG2」に関する運用上のベストプラクティス • CIS の「Critical Security Controls v8 IG3」に関する運用上のベストプラクティス • AWS Well-Architected フレームワークのセキュリティの柱に関する運用上のベストプラクティス • 「Esquema Nacional de Seguridad (ENS) Low」に関する運用のベストプラクティス • 「Esquema Nacional de Seguridad (ENS) Medium」に関する運用のベストプラクティス • 「Esquema Nacional de Seguridad (ENS) High」に関する運用のベストプラクティス • シンガポール金融管理局の「Notice 655」の運用のベストプラクティス	2022 年 3 月 16 日

	• NIST の「1800-25」に関する運用のベストプラクティス	
セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーでは、 AWS CloudFormation に対する追加のアクセス権限がサポートされるようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2022 年 3 月 14 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config を更新します。 • バックアップ計画によって保護された aurora リソース • dynamodb-バックアップ計画によって保護されるリソース • バックアップ計画によって保護された EBS リソース • EC2-バックアップ計画によって保護されるリソース • バックアップ計画によって保護された efs リソース • fsx-リソース-バックアップ計画によって保護される • rds-バックアップ計画によって保護されるリソース	2022 年 3 月 10 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Elastic Container Registry Public リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 3 月 4 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Elastic Compute Cloud リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 2 月 28 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • codedeploy-auto-rollback-monitor-enabled • codedeploy-ec2-minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-disabled	2022 年 2 月 25 日

AWS Config 更新時のログ記録とモニタリング	このリリースでは、 は Amazon EventBridge Events AWS Config でのモニタリングページ AWS Config を更新し、Amazon CloudWatch Events への参照を置き換えます。イベントを管理するには、Amazon EventBridge が好ましい方法です。CloudWatch Events と EventBridge は同じ基盤となるサービスと API ですが、EventBridge はより多くの機能を提供します。CloudWatch または EventBridge のいずれかで行った変更は、各コンソールに表示されます。詳細については、Amazon EventBridgeを参照してください。	2022 年 2 月 24 日
AWS の SDK ページ AWS Config	このリリースでは、 SDK で AWS Config を使用する が導入されました。 AWS ソフトウェア開発キット (SDKs) は、多くの一般的なプログラミング言語で利用できます。AWS ConfigAWS各 SDK には、デベロッパーが好みの言語でアプリケーションを簡単に構築できるようにする API、コード例、およびドキュメントが提供されています。	2022 年 2 月 24 日

セキュリティ IAM ロール信頼ポリシーの更新	このリリースでは、 は IAM 信頼ポリシーステートメント AWS Config を更新して、(AWS STS) オペレーション`sourceAccountId` の `sourceARN` および/または によるアクセスを制限するセキュリティ保護を信頼ポリシーに含めます AWS Security Token Service 。これにより、期待されるユーザーとシナリオのためにのみ、IAM ロールの信頼ポリシーがリソースにアクセスするようになります。 次のページが更新されます。 • ロールへの IAM 信頼ポリシーの追加	2022 年 2 月 18 日

グローバルリソースタイプの記録に対する変更	AWS Config は、新しいグローバルリソースタイプの AWS Config 記録方法を変更するようになりました。グローバルリソースタイプは、作成時にリージョンを指定する必要がない AWS リソースです。この変更が行われるまで、 AWS Configでサポートされるすべてのリージョンのグローバルリソースタイプの記録を有効にすることができました。 この変更後、 AWS Config 録画にオンボードされた新しいグローバルリソースタイプは、商用パーティションの場合はサービスのホームリージョンに、 AWS GovCloud (US) パーティションの場合は AWS GovCloud (米国西部) にのみ記録できます。これらの新しいグローバルリソースタイプの設定項目は、ホームリージョンおよび AWS GovCloud (米国西部) 以外では表示できなくなります。2022 年 2 月以降にオンボーディングされたグローバルリソースタイプのホームリージョンのリストについては、「すべてのサポートされているリソースタイプの記録」ページの表を参照してください。	2022 年 2 月 18 日

セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、Elastic Beanstalk 環境の詳細と、指定された Elastic Beanstalk 設定セットの設定内容の説明の取得、OpenSearch または Elasticsearch バージョンのマップの取得、データベースに利用できる Amazon RDS オプショングループの説明、および CodeDeploy デプロイ設定に関する情報の取得を実行する許可を付与するようになりました。また、このポリシーは AWS アカウント、 にアタッチされた指定された代替連絡先の取得、AWS Organizations ポリシーに関する情報の取得、Amazon ECR リポジトリポリシーの取得、アーカイブされた AWS Config ルールに関する情報の取得、Amazon ECS タスク定義ファミリーのリストの取得、指定された子 OUs) のリスト、指定されたターゲットルート、組織単位、またはアカウントにアタッチされたポリシーのリストを取得するアクセス許可を付与するようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2022 年 2 月 10 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-check • codebuild-project-logging-enabled • codebuild-project-s3-logs-encrypted • ec2-security-group-attached-to-eni-periodic • ecr-private-image-scanning-enabled • ecr-private-tag-immutability-enabled • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-hard-limit • ecs-task-definition-nonroot-user • ecs-task-definition-pid-mode-check • eks-cluster-oldest-supported-version	2022 年 2 月 10 日

	• eks-cluster-supported-version • lambda-vpc-multi-az-check • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-not-empty • rds-cluster-default-admin-check • rds-db-security-group-not-allowed • rds-instance-default-admin-check • redshift-default-admin-check • s3-bucket-acl-prohibited • s3-version-lifecycle-policy-check • waf-global-webacl-not-empty	
セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーで、Amazon CloudWatch ロンググループおよびストリームを作成し、作成したログストリームにログを書き込むアクセス許可が付与されるようになりました。詳細については、「AWS ConfigのAWS マネージドポリシー」を参照してください。	2022 年 2 月 2 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-tolerance • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-encryption-check	2022 年 1 月 31 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して AWS CodeDeploy リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2022 年 1 月 5 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon SageMaker AI リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2021 年 12 月 20 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • SME 向け ENISA サイバーセキュリティガイドの運用上のベストプラクティス	2021 年 12 月 20 日
AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • NIST 800 172 運用のベストプラクティス • NIST 800 181 運用のベストプラクティス 次のコンフォーマンスパックが更新されました。 • K-ISMS の運用のベストプラクティス	2021 年 11 月 18 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • Amazon API Gateway 運用のベストプラクティス • の運用上のベストプラクティス AWS Backup • CISA Cyber Essentials に関する運用上のベストプラクティス • DevOPs 運用のベストプラクティス • NIST プライバシーフレームワーク v1.0 オペレーションのベストプラクティス 次のコンフォーマンスパックが更新されました: • FedRAMP (Low) の運用のベストプラクティス • 「FedRAMP(Moderate)」に関する運用のベストプラクティス	2021 年 10 月 29 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して新しい Amazon OpenSearch Service リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2021 年 10 月 12 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config を更新します。 • MAS TRMGの運用のベストプラクティス	2021 年 10 月 12 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config を更新します。 • ABS CCIG 2.0 マテリアルワークロードに関する運用上のベストプラクティス • ABS CCIG 2.0 標準ワークロードに関する運用上のベストプラクティス • ACSC の Essential 8 に関する運用上のベストプラクティス • ACSC の「ISM」に関する運用上のベストプラクティス • BNM の「RMiT」に関する運用上のベストプラクティス • CMMC Level 1 に関する運用上のベストプラクティス • CMMC Level 2 に関する運用上のベストプラクティス • CMMC Level 3 に関する運用上のベストプラクティス • CMMC Level 4 に関する運用上のベストプラクティス • CMMC Level 5 に関する運用上のベストプラクティス • FDA Title 21 CFR Part 11 の運用のベストプラクティス • FFIEC に関する運用上のベストプラクティス	2021 年 9 月 30 日

	• シンガポール金融管理局の「Notice 655」の運用のベストプラクティス • NBC の「TRMG」の運用のベストプラクティス • NERC CIP に関する運用上のベストプラクティス • NIST 800-53 rev 5の運用のベストプラクティス	
セキュリティ IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーでは、Amazon OpenSearch Service (OpenSearch Service) のドメイン/ドメインの詳細を取得する権限と、特定の Amazon Relational Database Service (Amazon RDS) DB パラメータグループの詳細なパラメータリストを取得する権限が付与されるようになりました。このポリシーでは、Amazon ElastiCache スナップショットの詳細を取得するアクセス許可を付与します。詳細については、[AWS の AWS Config管理ポリシー] を参照してください。	2021 年 9 月 8 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して、新しい Amazon Elastic Compute Cloud リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2021 年 9 月 7 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config を更新します。 • APRA の「CPG 234」に関する運用上のベストプラクティス • CIS AWS Foundations Benchmark v1.4 レベル 1 の運用上のベストプラクティス • CIS AWS Foundations Benchmark v1.4 Level 2 の運用上のベストプラクティス • NCSC Cloud Security Principles に関する運用上のベストプラクティス • NCSC の「Cyber Assesment Framework」に関する運用上のベストプラクティス • NIST 800 171 に関する運用上のベストプラクティス • NIST の「CSF」に関する運用上のベストプラクティス • RBI の「Cyber Security Framework for UCBs」に関する運用上のベストプラクティス • RBI の「MD-ITF」の運用のベストプラクティス • NYDFS 23 の運用のベストプラクティス	2021 年 8 月 30 日

	• PCI DSS 3.2.1 運用のベストプラクティス	
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • バックアップ計画によって保護された aurora リソース • バックアップ計画-分-頻度と分保持チェック • バックアップ/リカバリ・ポイント暗号化 • バックアップ/リカバリ・ポイントの手動削除/無効化 • バックアップ/リカバリ・ポイントの最小保存期間チェック • dynamodb-バックアップ計画によって保護されるリソース • バックアップ計画によって保護された EBS リソース • EC2-バックアップ計画によって保護されるリソース • バックアップ計画によって保護された efs リソース • fsx-リソース-バックアップ計画によって保護される • rds-バックアップ計画によって保護されるリソース	2021 年 8 月 20 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • NZISM 運用のベストプラクティス	2021 年 8 月 20 日
セキュリティ Amazon SNS ポリシーの更新	このリリースでは、 は、サービスにリンクされたロールを使用してトピックポリシーで `sourceARN` および/または へのアクセスを制限するセキュリティ保護を含めるときに、Amazon SNS トピック`sourceAccountId` の IAM ポリシーステートメント AWS Config を更新します。これにより、Amazon SNS が期待されるユーザーとシナリオのみに代わってリソースにアクセスしていることを確認できます。 次のページが更新されます。 • Amazon SNS トピックへの許可	2021 年 8 月 17 日

セキュリティ AWS Lambda ポリシーの更新	このリリースでは、 はカスタムルールの AWS Lambda AWS Config リソースベースのポリシー AWS Config を更新して、 `sourceARN` および/または呼び出しリクエスト`sourceAccountId` でアクセスを制限するセキュリティ保護を含めます。これにより、 AWS Lambda が想定ユーザーおよびシナリオのみに代わって リソースにアクセスできるようになります。 次のページが更新されます。 • AWS::Config::ConfigRule • のカスタムルールの開発 AWS Config	2021 年 8 月 12 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して Amazon Kinesis リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2021 年 8 月 6 日

AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • 「Esquema Nacional de Seguridad (ENS) High」に関する運用のベストプラクティス 次のコンフォーマンスパックが更新されました: • AWS Well-Architected フレームワークの信頼性の柱に関する運用上のベストプラクティス • AWS Well-Architected フレームワークのセキュリティの柱に関する運用上のベストプラクティス • 「Esquema Nacional de Seguridad (ENS) Low」に関する運用のベストプラクティス • 「Esquema Nacional de Seguridad (ENS) Medium」に関する運用のベストプラクティス • HIPAA Security の運用のベストプラクティス	2021 年 7 月 30 日

AWS Config カスタムルールの AWS Lambda 関数の例	このリリースでは、 はAWS Config ルールの関数の例 (Python) で Python AWS Lambda 関数の例 AWS Config を提供します。	2021 年 7 月 29 日

セキュリティの IAM 更新	`AWSConfigServiceRolePolicy` ポリシーおよび `AWS_ConfigRole` ポリシーでは、ロググループのタグの一覧表示、ステートマシンのタグの一覧表示、すべてのステートマシンの一覧表示を行うアクセス許可が付与されるようになりました。これらのポリシーは、ステートマシンに関する詳細を取得するアクセス許可を付与するようになりました。これらのポリシーでは、Amazon EC2 Systems Manager (SSM)、Amazon Elastic Container Registry、Amazon FSx、Amazon Data Firehose、Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon Relational Database Service (Amazon RDS)、Amazon Route 53、Amazon SageMaker AI、Amazon Simple Notification Service AWS Database Migration Service AWS Global Accelerator、および に対する追加のアクセス許可もサポートされるようになりました AWS Storage Gateway。詳細については、AWS ConfigのAWS 管理ポリシーを参照してください。	2021 年 7 月 28 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して AWS Backup リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2021 年 7 月 14 日
AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は次のコンフォーマンスパック AWS Config をサポートしています。 • CIS の「Critical Security Controls v8 IG1」に関する運用上のベストプラクティス • CIS の「Critical Security Controls v8 IG2」に関する運用上のベストプラクティス • CIS の「Critical Security Controls v8 IG3」に関する運用上のベストプラクティス • NIST の「1800 25」に関する運用上のベストプラクティス	2021 年 7 月 9 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • ssm-document-not-public • s3-account-level-public-access-blocks-periodic	2021 年 6 月 25 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • ec2-instance-multiple-eni-check • elbv2-acm-certificate-required • autoscaling-launch-config-public-ip-disabled	2021 年 6 月 10 日

セキュリティの IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、IAM Access Analyzer に関する AWS Systems Manager ドキュメントと情報のアクセス許可を表示するアクセス許可を付与するようになりました。これらのポリシーは、Amazon Kinesis、Amazon ElastiCache、Amazon EMR AWS Network Firewall、Amazon Route 53、Amazon Relational Database Service (Amazon RDS) の追加 AWS リソースタイプをサポートするようになりました。これらのアクセス許可の変更により AWS Config 、 はこれらのリソースタイプをサポートするために必要な読み取り専用 APIs を呼び出すことができます。これらのポリシーでは、lambda-inside-vpc マネージドルールの Lambda@ AWS Config Edge 関数のフィルタリングもサポートされるようになりました。詳細については、AWS の [AWS Config管理ポリシー] を参照してください。	2021 年 6 月 8 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-enabled • api-gw-associated-with-waf • iam-policy-no-statements-with-full-access	2021 年 5 月 19 日
AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して Amazon Elastic File System リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2021 年 5 月 13 日

セキュリティの IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、 API Gateway の Config ルールをサポートするために、 API Gateway への読み取り専用 GET 呼び出しを AWS Config に許可するアクセス許可を付与するようになりました。これらのポリシーには、 が新しい`AWS::S3::AccessPoint` リソースタイプをサポートするために必要な Amazon Simple Storage Service (Amazon S3) 読み取り専用 APIs を AWS Config 呼び出すためのアクセス許可も追加されています。詳細については、[AWS の AWS Config管理ポリシー] を参照してください。	2021 年 5 月 10 日
AWS Config カスタムルール	デベロッパーガイドの次のページが更新されました: • のカスタムルールの開始方法 AWS Config • のカスタムルールの開発 AWS Config	2021 年 4 月 30 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • aurora-mysql-backtracking-enabled • ec2-instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-upgrade-enabled • redshift-enhanced-vpc-routing-enabled	2021 年 4 月 15 日

セキュリティの IAM 更新	`AWSConfigServiceRolePolicy` ポリシーと `AWS_ConfigRole` ポリシーは、 AWS Systems Manager 指定されたドキュメントに関する情報を表示するアクセス許可を付与するようになりました。これらのポリシーでは、Amazon Elastic File System AWS Backup、Amazon ElastiCache、Amazon Simple Storage Service (Amazon S3)、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Kinesis、Amazon SageMaker AI AWS Database Migration Service、Amazon Route 53 の追加 AWS リソースタイプもサポートされるようになりました。これらのアクセス許可の変更により AWS Config 、はこれらのリソースタイプをサポートするために必要な読み取り専用 APIs を呼び出すことができます。詳細については、[AWS の AWS Config管理ポリシー] を参照してください。	2021 年 4 月 14 日

設定項目 (CI) としてのコンフォーマンスパックのコンプライアンス	このリリースでは、 はコンフォーマンスパックのコンプライアンスを設定項目として AWS Config サポートしています。これにより、以下を行うことができます: • コンフォーマンスパックのコンプライアンス状態に対する変更のタイムラインを表示する • 複数のアカウントとリージョンにまたがるコンフォーマンスパックのコンプライアンスをまとめる • 高度なクエリを使用してコンフォーマンスパックのコンプライアンスを確認する 次のデータ型が更新されました。 • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary デベロッパーガイドの次のページが更新されました: • コンフォーマンスパックのダッシュボードでのコンプライアンスデータの表示	2021 年 3 月 30 日

	• コンフォーマンスパックのコンプライアンス履歴のタイムラインの表示 • アグリゲータダッシュボードでのコンプライアンスデータの表示 • AWS リソースの現在の設定状態のクエリ • サポートされているリソースタイプ	
ページ割りの更新	このリリースでは、 AWS Config 高度なクエリ機能が、COUNT や SUM などの集計関数を含むクエリのページ分割をサポートするようになりました。高度なクエリを使用して、以前は 500 行に制限されていたページ割りを介して集計クエリの完全な結果を取得できるようになりました。詳細については、AWS 「リソースの現在の設定状態のクエリ」を参照してください。	2021 年 3 月 26 日
リージョンのサポート	このリリースでは、 AWS Config AWS Config ルールがアジアパシフィック (大阪) リージョンでサポートされるようになりました。	2021 年 3 月 4 日

AWS Config が新しいリソースタイプをサポート	このリリースでは、 AWS Config を使用して Amazon Elastic Container Registry、Amazon Elastic Container Service、Amazon Elastic Kubernetes Service リソースタイプの設定変更を記録できます。詳細については、[サポートされるリソースタイプ] を参照してください。	2021 年 2 月 25 日
KMS 暗号化のサポート	このリリース AWS Config では、 により S3 バケット配信 AWS Config のために によって配信されるオブジェクトに対して KMS ベースの暗号化を使用できます。 次のデータ型が更新されました。 • DeliveryChannel • PutDeliveryChannel デベロッパーガイドの次のページが更新されました: • KMS キーのアクセス許可 • に割り当てられた IAM ロールのアクセス許可 AWS Config	2021 年 2 月 16 日

AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	2021 年 2 月 16 日
保存されたクエリリージョンのサポート	このリリースでは、保存されたクエリが AWS GovCloud (米国東部) および AWS GovCloud (米国西部) リージョンでサポートされるようになりました。	2021 年 2 月 15 日
マルチアカウントマルチリージョンのデータ集約のリージョンをサポート	このリリースでは、マルチアカウントマルチリージョンのデータ集約が、アフリカ (ケープタウン) および欧州 (ミラノ) のリージョンでもサポートされます。詳細については、[マルチアカウントマルチリージョンのデータ集約] を参照してください。	2021 年 2 月 15 日
高度なクエリリージョンのサポート	このリリースでは、アフリカ (ケープタウン) および欧州 (ミラノ) のリージョンでも高度なクエリがサポートされます。詳細については、AWS 「リソースの現在の設定状態のクエリ」を参照してください。	2021 年 2 月 15 日

AWS Config RSS フィードで利用可能なドキュメント履歴通知	RSS フィードをサブスクライブすることで、 AWS Config ドキュメントの更新に関する通知を受信できるようになりました。	2021 年 1 月 1 日

以前の更新

次の表は、2020 年 12 月 31 AWS Config 日以前の のドキュメントリリース履歴を示しています。

変更	説明	リリース日
保存されたクエリのサポート	このリリース AWS Config では、 でクエリを保存できます。クエリを保存すると、クエリの検索、クエリエディタへのコピー、編集、削除を行うことができます。クエリを保存する方法の詳細については、[の SQL クエリエディタを使用したクエリ AWS Config （コンソール） および の AWS Config SQL クエリエディタを使用したクエリ (AWS CLI)] を参照してください。 API の詳細については、「AWS Config API リファレンス」を参照してください。 • PutStoredQuery • GetStoredQuery • ListStoredQueries • DeleteStoredQuery また、「のサービスの制限 AWS Config」も参照してください。	2020 年 12 月 21 日

変更	説明	リリース日
プロセスチェックのサポート	このリリースでは、 は、コンフォーマンスパックの一部として検証が必要な外部タスクと内部タスクを追跡できる AWS Config ルールの一種であるプロセスチェック AWS Config をサポートします。プロセスチェックを使用すると、要件とアクションのコンプライアンスを 1 か所で一覧表示できます。 プロセスチェックの詳細については、AWS Config のコンフォーマンスパック内のプロセスチェック AWS Config トピックおよび [PutExternalEvaluation API] を参照してください。	2020 年 12 月 17 日

変更	説明	リリース日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-enabled • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-enabled • rds-cluster-iam-authentication-enabled • redshift-cluster-kms-enabled • s3-bucket-level-public-access-prohibited • subnet-auto-assign-public-ip-disabled • vpc-network-acl-unused-check	2020 年 12 月 17 日
AWS Config がをサポート AWS Network Firewall	このリリースでは、 AWS Config を使用して、 AWS Network Firewall FirewallPolicy、RuleGroup、および Firewall リソースタイプの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2020 年 12 月 4 日

変更	説明	リリース日
ドキュメントの更新	AWS Config は、委任管理者アカウントで組織全体のリソースデータ集約のサポートを追加しました。委任管理者アカウントを使用して、 AWS 組織のすべてのメンバーアカウントを対象に、リソース構成とコンプライアンスデータを集約することができるようになりました。 詳細については、[PutConfigurationAggregator]、[のアグリゲータの作成 AWS Config] および [の委任管理者の登録 AWS Config] を参照してください。	2020 年 12 月 4 日
AWS Config が新しいコンフォーマンスパックをサポート	• 「Esquema Nacional de Seguridad (ENS) Low」に関する運用のベストプラクティス • 「Esquema Nacional de Seguridad (ENS) Medium」に関する運用のベストプラクティス • NCSC の「Cyber Assesment Framework」に関する運用上のベストプラクティス • RBI の「Cyber Security Framework for UCBs」に関する運用上のベストプラクティス	2020 年 10 月 30 日

変更	説明	リリース日
AWS Config が新しいコンフォーマンスパックをサポート	• ACSC の Essential 8 に関する運用上のベストプラクティス • ACSC の「ISM」に関する運用上のベストプラクティス • AI と機械学習に関する運用面のベストプラクティス • アセット管理に関する運用上のベストプラクティス • BCP と DR に関する運用上のベストプラクティス • EC2 に関する運用上のベストプラクティス • K-ISMS の運用のベストプラクティス • ロードバランシングの運用のベストプラクティス • ログ記録に関する運用上のベストプラクティス • モニタリングの運用のベストプラクティス • サーバーレスの運用のベストプラクティス	2020 年 10 月 22 日

変更	説明	リリース日
AWS Config が新しいコンフォーマンスパックをサポート	• APRA の「CPG 234」に関する運用上のベストプラクティス • FedRAMP (Low) の運用のベストプラクティス • シンガポール金融管理局の「Notice 655」の運用のベストプラクティス • NBC の「TRMG」の運用のベストプラクティス • NCSC Cloud Security Principles に関する運用上のベストプラクティス • RBI の「MD-ITF」の運用のベストプラクティス	2020 年 10 月 15 日

変更	説明	リリース日
AWS Config が新しいコンフォーマンスパックをサポート	• ABS CCIG 2.0 マテリアルワークロードに関する運用上のベストプラクティス • ABS CCIG 2.0 標準ワークロードに関する運用上のベストプラクティス • BNM の「RMiT」に関する運用上のベストプラクティス • データの回復性に関する運用上のベストプラクティス • データレイクと分析サービスに関する運用上のベストプラクティス • 暗号化とキー管理に関する運用上のベストプラクティス • FDA Title 21 CFR Part 11 の運用のベストプラクティス • パブリックにアクセス可能なリソースの運用のベストプラクティス • MAS TRMGの運用のベストプラクティス • NERC CIP BCSI に関する運用上のベストプラクティス • NYDFS 23 の運用のベストプラクティス	2020 年 10 月 8 日

変更	説明	リリース日
AWS Config が新しいコンフォーマンスパックをサポート	• AWS Well-Architected フレームワークの信頼性の柱に関する運用上のベストプラクティス • AWS Well-Architected フレームワークのセキュリティの柱に関する運用上のベストプラクティス • コンピューティングサービスに関する運用上のベストプラクティス • データベースサービスに関する運用上のベストプラクティス • サービスの管理およびガバナンスの運用のベストプラクティス • ネットワークおよびコンテンツ配信サービスの運用のベストプラクティス • セキュリティ、ID、コンプライアンスの運用のベストプラクティス • ストレージサービスの運用のベストプラクティス	2020 年 10 月 26 日
AWS Config が新しいコンフォーマンスパックをサポート	• FedRAMP(Moderate) に関する運用上のベストプラクティス • FFIEC に関する運用上のベストプラクティス • HIPAA Security の運用のベストプラクティス • NIST の「800-53 rev 4」の運用のベストプラクティス • NIST 800 171 に関する運用上のベストプラクティス	2020 年 9 月 28 日

変更	説明	リリース日
ドキュメントの更新	次のコンフォーマンスパックのトピックが更新されました。 • のコンフォーマンスパックの前提条件 AWS Config • のコンフォーマンスパックのデプロイ AWS Config • 組織内のすべての AWS Config アカウントにおける のコンフォーマンスパックの管理	2020 年 9 月 28 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • iam-customer-policy-blocked-kms-actions • iam-inline-policy-blocked-kms-actions	2020 年 9 月 17 日
AWS Config v2 AWS WAFをサポート	このリリースでは、 AWS Config を使用して、 AWS WAF v2 WebACL、IPSet、RegexPatternSet、RuleGroup、および ManagedRuleSet リソースタイプの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2020 年 9 月 1 日

変更	説明	リリース日
ドキュメントの更新	フルアクセスを許可するカスタムアクセス許可の作成について、ノートが へのフルアクセス AWS Config に追加されました。 以下のルールのドキュメントが更新されました。 • s3-bucket-server-side-encryption-enabled • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-platform-check	2020 年 8 月 24 日
ドキュメントの更新	PCI DSS 3.2.1 運用のベストプラクティス および NIST の「CSF」に関する運用上のベストプラクティス テンプレートが更新されました。	2020 年 8 月 14 日
ドキュメントの更新	リレーションシップクエリの例が追加されました。詳細については、「AWS Configの関係クエリの例」を参照してください。	2020 年 7 月 30 日

変更	説明	リリース日
ドキュメントの更新	次のデータ型が更新されました。 • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus	2020 年 7 月 23 日
AWS Config が AWS Systems Manager リソースタイプをサポート	このリリースでは、 AWS Config を使用して AWS Systems Manager ファイルデータリソースタイプの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2020 年 7 月 9 日
ドキュメントの更新	AWS Identity and Access Management に関する運用上のベストプラクティス および PCI DSS 3.2.1 運用のベストプラクティス テンプレートが更新されました。	2020 年 7 月 9 日

変更	説明	リリース日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • account-part-of-organizations • alb-http-drop-invalid-header-enabled • alb-waf-enabled • cloudfront-default-root-object-configured • cloudfront-origin-access-identity-enabled • cloudfront-origin-failover-enabled • cloudfront-sni-enabled • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-check • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-access • eks-secrets-encrypted • elasticsearch-node-to-node-encryption-check • elb-cross-zone-load-balancing-enabled • elb-tls-https-listeners-only • iam-no-inline-policy-check	2020 年 7 月 9 日

変更	説明	リリース日
	• rds-cluster-deletion-protection-enabled • rds-in-backup-plan • rds-instance-deletion-protection-enabled • rds-instance-iam-authentication-enabled • rds-logging-enabled • redshift-backup-enabled • waf-classic-logging-enabled • wafv2-logging-enabled 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	
マルチアカウントマルチリージョンのデータ集約のリージョンをサポート	このリリースでは、マルチアカウントマルチリージョンのデータ集約が、アジアパシフィック (香港) および中東 (バーレーン) のリージョンでサポートされるようになりました。詳細については、[Multi-Account Multi-Region Data Aggregation] および [のマルチアカウントマルチリージョンデータ集約のトラブルシューティング AWS Config] を参照してください。	2020 年 7 月 1 日

変更	説明	リリース日
高度なクエリリージョンのサポート	このリリースでは、高度なクエリがアジアパシフィック (香港) および中東 (バーレーン) のリージョンでサポートされるようになりました。詳細については、「を使用したリソースの AWS 現在の設定状態のクエリ AWS Config」を参照してください。	2020 年 7 月 1 日
ドキュメントの更新	以下のルールのドキュメントが更新されました。 • ec2-managedinstance-association-compliance-status-check • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • rds-snapshots-public-prohibited • s3-bucket-policy-grantee-check	2020 年 6 月 30 日
ドキュメントの更新	ドキュメントは、 のセキュリティに関する情報で更新されました AWS Config。「のセキュリティ AWS Config」を参照してください。	2020 年 6 月 24 日
ドキュメントの更新	AWS Control Tower Detective Guardrails Conformance Pack テンプレートが更新されました。詳細については、「AWS Control Tower Detective ガードレールコンフォーマンスパック」を参照してください。	2020 年 6 月 4 日

変更	説明	リリース日
AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は NIST CSF コンフォーマンスパックの運用上のベストプラクティス AWS Config をサポートしています。詳細については、「NIST の「CSF」に関する運用上のベストプラクティス 」を参照してください。	2020 年 5 月 29 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec2-ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s3-bucket-default-lock-enabled • s3-default-encryption-kms • securityhub-enabled • sns-encrypted-kms 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2020 年 5 月 28 日

変更	説明	リリース日
遅延管理者のサポート	このリリースでは、管理アカウントに加えて、組織内の任意の委任メンバーアカウントから AWS Config ルールとコンフォーマンスパックをデプロイできます。 API の詳細については、「AWS Config API リファレンス」を参照してください。 • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus 詳細については、「のサービスの制限 AWS Config」を参照してください。	2020 年 5 月 27 日

変更	説明	リリース日
AWS Config ルールリージョンのサポート	このリリースでは、アフリカ (ケープタウン) および欧州 (ミラノ) リージョンでサポートされている AWS Config ルールはほとんどありません。ルールとそのサポートされているリージョンの詳細なリストについては、[AWS Config マネージドルールのリスト] を参照してください。	2020 年 4 月 28 日
AWS Config が新しいコンフォーマンスパックをサポート	このリリースでは、 は 2 つのコンフォーマンスパック AWS Config をサポートしています。 • AWS Control Tower Detective ガードレールコンフォーマンスパック • CIS 運用のベストプラクティス 詳細については、「のコンフォーマンスパックのサンプルテンプレート AWS Config」を参照してください。	2020 年 4 月 22 日
AWS Config が AWS Secrets Manager をサポート	このリリースでは、 AWS Config を使用して Secrets Manager シークレットの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2020 年 4 月 20 日

変更	説明	リリース日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-check 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2020 年 4 月 16 日
コンフォーマンスパックリージョンのサポート	このリリースでは、コンフォーマンスパックが、アジアパシフィック (香港) および中東 (バーレーン) でサポートされるようになりました。詳細については、「Conformance Packs」を参照してください。	2020 年 4 月 8 日
ドキュメントの更新	AWS Config の制限は、このデベロッパーガイドで確認できます。詳細については、「のサービスの制限 AWS Config」を参照してください。	2020 年 4 月 8 日
ドキュメントの更新	AWS CloudFormation レジストリを通じて管理 (created/updated/deleted されるサードパーティーリソースは、 で設定項目 AWS Config として自動的に追跡されます。詳細については、「を使用したサードパーティーリソース AWS Config の による設定の記録 AWS CLI」を参照してください。	2020 年 3 月 30 日

変更	説明	リリース日
ドキュメントの更新	AWS Config マネージドルールが更新され、情報が含まれます AWS リージョン 。詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2020 年 3 月 27 日
AWS Config が Amazon SNS リソースタイプをサポート	このリリースでは、 AWS Config を使用して Amazon SNS トピックの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2020 年 3 月 6 日
マルチアカウントマルチリージョンのデータ集約のリージョンをサポート	このリリースでは、マルチアカウントマルチリージョンのデータ集約が、新しく欧州 (ストックホルム) リージョンでサポートされるようになりました。詳細については、「Multi-Account Multi-Region Data Aggregation」を参照してください。	2020 年 3 月 5 日
高度なクエリリージョンのサポート	このリリースでは、欧州 (ストックホルム) リージョンで高度なクエリがサポートされるようになりました。詳細については、「を使用したリソースの AWS 現在の設定状態のクエリ AWS Config」を参照してください。	2020 年 3 月 5 日

変更	説明	リリース日
AWS Config では、設定アグリゲータを使用して高度なクエリを実行できます。	このリリースでは、 が設定アグリゲータを使用してリソース設定プロパティに基づいて高度なクエリを実行するサポート AWS Config を追加し、複数のアカウントとリージョンで同じクエリを実行できます。詳細については、「を使用したリソースの AWS 現在の設定状態のクエリ AWS Config」を参照してください。 このリリースでは、 は `SelectAggregateResourceConfig` API AWS Config を追加します。詳細については、「AWS Config API リファレンス」の [SelectAggregateResourceConfig] を参照してください。	2020 年 2 月 28 日
AWS Config が Amazon SQS リソースタイプをサポート	このリリースでは、 AWS Config を使用して Amazon SQS キューの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2020 年 2 月 13 日

変更	説明	リリース日
AWS CloudFormation コンフォーマンスパックのサポート	このリリースでは、 `AWS::Config::ConformancePack` および のリソース AWS CloudFormation のサポートが追加されました`OrganizationConformancePack` 。 • AWS::Config::ConformancePack `AWS::Config::ConformancePack` リソースを使用して、アカウントとリージョン、および AWS 組織全体に簡単にデプロイできるルールの AWS Config コレクションであるコンフォーマンスパックを作成します。 • AWS::Config::OrganizationConformancePack `AWS::Config::OrganizationConformancePack` リソースを使用して、 に関する情報を含む Organization Conformance Pack を作成します。 がメンバーアカウントで AWS Config 作成するコンフォーマンスパック。	2020 年 2 月 13 日

変更	説明	リリース日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • api-gw-execution-logging-enabled • ec2-stopped-instance • elasticache-redis-cluster-automatic-backup-check • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • s3-account-level-public-access-blocks • sagemaker-endpoint-configuration-kms-key-configured • service-vpc-endpoint-enabled 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2019 年 12 月 20 日

変更	説明	リリース日
カスタムリソースタイプの設定の記録	このリリースでは、 がカスタムリソースタイプの設定を記録するサポート AWS Config を導入しました。コンソール AWS Config と APIs を使用して AWS Config 、サードパーティーリソースの設定データを に公開し、リソースインベントリと設定履歴を表示およびモニタリングできます。詳細については、「を使用したサードパーティーリソース AWS Config の による設定の記録 AWS CLI」を参照してください。 API の詳細については、「AWS Config API リファレンス」を参照してください。 • DeleteResourceConfig • PutResourceConfig	2019 年 11 月 20 日

変更	説明	リリース日
コンフォーマンスパック	このリリースでは、 AWS Config にコンフォーマンスパックが導入されました。コンフォーマンスパックを使用すると、 AWS Config ルールと修復アクションのコレクションをパッケージ化し、 AWS 組織全体に単一のエンティティとしてデプロイできます。詳細については、「Conformance Packs」を参照してください。 API の詳細については、「AWS Config API リファレンス」を参照してください。 • DeleteOrganizationConformancePack • DeleteOrganizationConformancePack • DescribeConformancePacks • DescribeConformancePacks • DescribeConformancePackStatus • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetConformancePackComplianceDetails • GetConformancePackComplianceSummary • GetOrganizationConformancePackDetailedStatus • PutConformancePack	2019 年 11 月 19 日

変更	説明	リリース日
	• PutOrganizationConformancePack	
AWS Config が Amazon OpenSearch Service と AWS Key Management Service リソースタイプをサポート	このリリースでは、 AWS Config を使用して Amazon OpenSearch Service ドメインと AWS Key Management Service キーの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2019 年 11 月 11 日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-only • kms-cmk-not-scheduled-for-deletion • sagemaker-notebook-no-direct-internet-access • sagemaker-notebook-instance-kms-key-configured • shield-drt-access 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2019 年 10 月 10 日

変更	説明	リリース日
AWS Config が Amazon RDS リソースタイプをサポート	このリリースでは、 AWS Config を使用して Amazon Relational Database Service (Amazon RDS) DBCluster と DBClusterSnapshot の設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2019 年 9 月 17 日
AWS Config が Amazon QLDB リソースタイプをサポート	このリリースでは、 AWS Config を使用して Amazon Quantum 台帳データベース (QLDB) 台帳リソースタイプの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2019 年 9 月 10 日

変更	説明	リリース日
AWS Config では、 AWS Config ルールによって評価される非準拠リソースに自動修復を適用できます。	このリリースでは、 AWS Config ルールによって評価される非準拠リソースに AWS Systems Manager 自動化ドキュメントを使用して自動修復を適用するサポート AWS Config が導入されました。詳細については、「を使用した非準拠リソースの修復 AWS Config」を参照してください。 このリリースでは、 は次の新しい APIs AWS Config を追加します。詳細については、「AWS Config API リファレンス」を参照してください。 • PutRemediationExceptions • DescribeRemediationExceptions • DeleteRemediationExceptions	2019年9月5日

変更	説明	リリース日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config をサポートしています。 • alb-http-to-https-redirection-check • api-gw-cache-enabled-and-encrypted • api-gw-endpoint-type-check • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-check • elb-deletion-protection-enabled • lambda-concurrency-check • lambda-dlq-check • lambda-inside-vpc • shield-advanced-enabled-autorenew • vpc-vpn-2-tunnels-up 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2019 年 8 月 22 日

変更	説明	リリース日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config を更新します。 • cloudfront-viewer-policy-https • ec2-instance-no-public-ip • ec2-security-group-attached-to-eni • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-check • vpc-sg-open-only-to-authorized-ports 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2019 年 7 月 31 日
AWS Config が Amazon EC2 リソースタイプをサポート	このリリースでは、 AWS Config を使用して、VPCEndpointC VPCEndpointService、VPCPeeringConnection の Amazon EC2 リソースの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2019 年 7 月 12 日

変更	説明	リリース日
AWS Config では、組織 AWS アカウント 内のすべての で AWS Config ルールを管理できます。	このリリース AWS Config では、 は組織 AWS アカウント 内のすべての でルールを管理する AWS Config ためのサポートを導入します。組織内のすべてのアカウントで AWS Config ルールを一元的に作成、更新、削除できます。詳細については、「組織内のすべてのアカウントでの AWS Config ルールの管理」を参照してください。 API の詳細については、「AWS Config API リファレンス」を参照してください。 • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule	2019 年 7 月 9 日
AWS Config が Amazon S3 および Amazon EC2 リソースタイプをサポート	このリリースでは、 AWS Config を使用して、Amazon S3 AccountPublicAccessBlock リソースと次の Amazon EC2 リソースの設定変更を記録できます。NatGateway、EgressOnlyInternetGateway、および FlowLog。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2019 年 5 月 17 日

変更	説明	リリース日
AWS Config マネージドルールの更新	このリリースでは、 は次のマネージドルール AWS Config を更新します。 • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2019 年 5 月 7 日
AWS Config では、 を使用して修復アクションを削除できます AWS Management Console。	このリリース AWS Config では、 を使用して修復アクションを削除するサポートが導入されています AWS Management Console。詳細については、「を使用した非準拠リソースの修復 AWS Config」を参照してください。	2019 年 4 月 24 日
AWS Config が新しいマネージドルールをサポート	このリリースでは新しいマネージドルール fms-shield-resource-policy-check をサポートしています。 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2019 年 4 月 7 日

変更	説明	リリース日
AWS Config が Amazon API Gateway リソースタイプをサポート	このリリースでは、 AWS Config を使用して、Api (WebSocket API)、RestApi (REST API)、Stage (WebSocket API ステージ) 、Stage (REST API ステージ) の各 Amazon API Gateway リソースの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2019 年 3 月 20 日
AWS Config では、高度なクエリを実行できます。	このリリースでは、リソース設定プロパティに基づいて高度なクエリを実行するサポートが AWS Config に追加されました。詳細については、「を使用したリソースの AWS 現在の設定状態のクエリ AWS Config」を参照してください。 このリリースでは、 は `SelectResourceConfig` API AWS Config を追加します。詳細については、「AWS Config API リファレンス」の [SelectResourceConfig] を参照してください。	2019 年 3 月 19 日

変更	説明	リリース日
AWS Config では、 AWS Config リソースにタグを割り当てることができます。	このリリース AWS Config では、と の 3 つの AWS Config リソースConfigRule, ConfigurationAggregator, に対するタグベースのアクセスコントロールのサポートが導入されましたAggregationAuthorization 。詳細については、「AWS Config リソースのタグ付け」を参照してください。 このリリースでは、次のデータ型を使用して、 AWS Config リソースのタグの追加、削除、一覧表示を行うことができます。詳細については、「AWS Config の API リファレンス」を参照してください。 • ListTagsForResource • TagResource • UntagResource	2019 年 3 月 14 日

変更	説明	リリース日
AWS Config では、 AWS Config ルールによって評価される非準拠のリソースに修復を適用できます。	このリリース AWS Config では、AWS Config ルールによって評価される非準拠リソースに AWS Systems Manager オートメーションドキュメントを使用して修復を適用するサポートが導入されました。詳細については、「を使用した非準拠リソースの修復 AWS Config」を参照してください。 このリリースでは、 は次の新しい APIs AWS Config を追加します。詳細については、「AWS Config API リファレンス」を参照してください。 • DeleteRemediationConfiguration • DescribeRemediationConfigurations • DescribeRemediationExecutionStatus • PutRemediationConfigurations • StartRemediationExecution	2019 年 3 月 12 日

変更	説明	リリース日
AWS Config が中国 (寧夏) リージョンで AWS Config ルールをサポート	このリリースでは、中国 (寧夏) リージョンの 54 AWS Config ルールのみがサポートされています。詳細については、「AWS Config マネージドルールのリスト」を参照してください。 ただし、現在、中国 (寧夏) リージョンでは以下のルール AWS Config はサポートされていません。 • acm-certificate-expiration-check • cmk-backing-key-rotation-enabled • cloudformation-stack-drift-detection-check • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-enabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-check	2019 年 3 月 12 日

変更	説明	リリース日
	• fms-webacl-rulegroup-association-check • guardduty-enabled-centralized • lambda-function-public-access-prohibited • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-enabled • root-account-mfa-enabled • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-grantee-check • s3-bucket-policy-not-more-p ermissive • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited • s3-bucket-server-side-encryption-enabled • s3-bucket-ssl-requests-only	
AWS Config が新しいマネージドルールをサポート	このリリースでは、以下の新しいマネージドルールをサポートしています。 • iam-user-mfa-enabled • s3-bucket-policy-grantee-check 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2019 年 1 月 21 日

変更	説明	リリース日
AWS Config が Service Catalog リソースタイプをサポート	このリリースでは、 AWS Config を使用して、CloudFromation 製品、プロビジョニング済み製品、ポートフォリオの Service Catalog リソースの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2019 年 1 月 11 日
サービスにリンクされた AWS Config ルールのサポート	このリリースでは、 は、アカウントに AWS Config ルールを作成するための他の AWS サービスをサポートする新しいマネージド設定ルール AWS Config を追加します。詳細については、「サービスにリンクされた AWS Config ルール」を参照してください。	2018 年 11 月 20 日

変更	説明	リリース日
AWS Config では、 リソースの設定データを集約できます。 AWS	このリリースでは、 AWS がリソースの設定データを集約するためのサポート AWS Config を導入しました。詳細については、「のアグリゲータダッシュボードでのコンプライアンスデータとインベントリデータの表示 AWS Config」を参照してください。 このリリースでは、 は次の新しい APIs AWS Config を追加します。詳細については、「AWS Config の API リファレンス」を参照してください。 • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceCounts • GetAggregateResourceConfig • ListAggregateDiscoveredResources	2018 年 11 月 19 日

変更	説明	リリース日
AWS Config が新しいマネージドルールをサポート	このリリースでは、以下の新しいマネージドルールをサポートしています。 • cloudformation-stack-drift-detection-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2018 年 11 月 19 日

変更	説明	リリース日
AWS Config が新しいマネージドルールをサポート	このリリースでは、以下の新しいマネージドルールをサポートしています。 • access-keys-rotated • cloud-trail-cloud-watch-logs-enabled • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • cmk-backing-key-rotation-enabled • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-check • iam-root-access-key-check • iam-user-unused-credentials-check • mfa-enabled-for-iam-console-access • multi-region-cloudtrail-enabled • root-account-hardware-mfa-enabled • vpc-flow-logs-enabled 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2018 年 11 月12 日

変更	説明	リリース日
AWS Config が新しいマネージドルールをサポート	このリリースでは、以下の新しいマネージドルールをサポートしています。 • dynamodb-table-encryption-enabled • elb-logging-enabled • rds-instance-public-access-check • vpc-default-security-group-closed 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2018 年 10 月 24 日
コンプライアンス履歴をサポート	このリリースでは、 は AWS Config ルールによって評価されたリソースのコンプライアンス履歴の保存をサポートする AWS Config ようになりました。詳細については、「リソースおよびルールのコンプライアンス履歴タイムラインの表示」を参照してください。	2018 年 10 月 18 日
マルチアカウントマルチリージョンのデータ集約のリージョンをサポート	このリリースでは、マルチアカウントマルチリージョンのデータ集約が、新しく 6 つのリージョンでサポートされるようになりました。詳細については、「Multi-Account Multi-Region Data Aggregation」を参照してください。	2018 年 10 月 4 日

変更	説明	リリース日
AWS Config が AWS Config ルール APIs アクションのリソースレベルのアクセス許可をサポート	このリリースでは、 は特定の AWS Config ルール API アクションのリソースレベルのアクセス許可 AWS Config をサポートします。サポートされている API の詳細については、[AWS Config ルール API アクションでサポートされているリソースレベルのアクセス許可] を参照してください。	2018 年 10 月 1 日
AWS Config が CodePipeline リソースタイプをサポート	このリリースでは、 AWS Config を使用して AWS CodePipeline リソースタイプの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2018 年 9 月 12 日

変更	説明	リリース日
AWS Config が新しいマネージドルールをサポート	このリリースでは、以下の新しいマネージドルールをサポートしています。 • ec2-instance-managed-by-systems-manager • ec2-managedinstance-association-compliance-status-check • ec2-managedinstance-patch-compliance-status-check • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-not-more-permissive 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2018 年 9 月 5 日
AWS Config が AWS Systems Manager リソースタイプをサポート	このリリースでは、 AWS Config を使用して、 AWS Systems Manager パッチコンプライアンスおよび関連付けコンプライアンスリソースタイプの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2018 年 8 月 9 日

変更	説明	リリース日
AWS Config では、 を使用して AWS Config データを削除できます。 AWS Management Console	このリリース AWS Config では、 を使用して保持期間のサポートを導入します AWS Management Console。では AWS Management Console、`ConfigurationItems` のカスタムデータ保持期間を選択できます。詳細については、「AWS Config データの削除」を参照してください。	2018 年 8 月 7 日
AWS Config が AWS Shield リソースタイプをサポート	このリリースでは、 AWS Config を使用して AWS Shield Protection リソースタイプの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2018 年 8 月 7 日
AWS Config supports AWS PrivateLink	このリリースでは、 は AWS PrivateLink AWS Config をサポートしており、Amazon Virtual Private Cloud (VPC) と AWS ネットワーク AWS Config 全体との間でデータをルーティングできます。詳細については、「インターフェイス Amazon VPC エンドポイント AWS Config での の使用」を参照してください。	2018 年 7 月 31 日

変更	説明	リリース日
AWS Config では、 AWS Config データを削除できます。	このリリース AWS Config では、 で保持期間のサポートが導入されています。 AWS Config では、 の保持期間を指定してデータを削除できますConfigurationItems 。詳細については、「AWS Config データの削除」を参照してください。 このリリースでは、 は次の新しい APIs AWS Config を追加します。詳細については、「AWS Config の API リファレンス」を参照してください。 • PutRetentionConfiguration • DescribeRetentionConfigurations • DeleteRetentionConfiguration	2018 年 5 月 25 日
AWS Config が新しいマネージドルールをサポート	このリリースでは、以下の 2 つの新しいマネージドルールをサポートしています。 • lambda-function-settings-check • s3-bucket-replication-enabled • iam-policy-blacklisted-check 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2018 年 5 月 10 日

変更	説明	リリース日
AWS Config が AWS X-Ray リソースタイプをサポート	このリリースでは、 AWS Config を使用して AWS X-Ray EncryptionConfig リソースタイプの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2018 年 5 月 1 日
AWS Config が AWS Lambda リソースタイプと 1 つの新しいマネージドルールをサポート	このリリースでは、 AWS Config を使用して AWS Lambda 関数リソースタイプの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。 また、このリリースでは、lambda-function-public-access-prohibited マネージドルールをサポートしています。詳細については、「AWS Config マネージドルール」を参照してください。	2018 年 4 月 25 日
AWS Config が AWS Elastic Beanstalk リソースタイプをサポート	このリリースでは、 AWS Config を使用して、 AWS Elastic Beanstalk アプリケーション、アプリケーションバージョン、環境リソースの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2018 年 24 月 4 日

変更	説明	リリース日
AWS Config が新しいマネージドルールをサポート	このリリースでは、以下の 2 つの新しいマネージドルールをサポートしています。 • fms-webacl-resource-policy-check • fms-webacl-rulegroup-association-check 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2018 年 4 月 4 日

変更	説明	リリース日
マルチアカウント、マルチリージョンのデータ集計	このリリースでは、 にマルチアカウントのマルチリージョンデータ集約 AWS Config が導入されました。この機能を使用すると、複数のアカウントまたは組織と複数のリージョンの AWS Config データをアグリゲータアカウントに集約できます。詳細については、「Multi-Account Multi-Region Data Aggregation」を参照してください。 このリリースでは、 は次の新しい APIs AWS Config を追加します。詳細については、「AWS Config の API リファレンス」を参照してください。 • PutConfigurationAggregator • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAuthorization • DescribeAggregationAuthorizations • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRule • DescribeConfigurationAggregators • DescribeConfigurationAggregatorSourcesStatus • DeleteAggregationAuthorization	2018 年 4 月 4 日

変更	説明	リリース日
	• DeleteConfigurationAggregator	
Amazon CloudWatch Events AWS Config によるモニタリング	このリリースでは、Amazon CloudWatch Events を使用して AWS Config 、イベントのステータスの変化を検出して対応します。 詳細については、「Amazon EventBridge AWS Config によるモニタリング」を参照してください。	2018 年 3 月 29 日
新しい API オペレーション	このリリースでは、 で BatchGetResourceConfig API のサポート AWS Config が追加され、1 つ以上のリソースの現在の状態をバッチ取得できるようになりました。	2018 年 3 月 20 日
AWS Config supports AWS WAF RuleGroup リソースタイプ	このリリースでは、 AWS Config を使用して AWS WAF RuleGroup および AWS WAF RuleGroup リージョンリソースの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2018 年 2 月 15 日

変更	説明	リリース日
AWS Config が新しいマネージドルールをサポート	このリリースでは、以下の新しいマネージドルールをサポートしています。 • elb-acm-certificate-required • elb-custom-security-policy-ssl-check • elb-predefined-security-policy-ssl-check • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • iam-group-has-users-check • s3-bucket-server-side-encryption-enabled 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2018 年 1 月 25 日
AWS Config が Elastic Load Balancing リソースタイプをサポート	このリリースでは、 AWS Config を使用して Elastic Load Balancing クラシックロードバランサーの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2017 年 11 月 17 日

変更	説明	リリース日
AWS Config が Amazon CloudFront と AWS WAF リソースタイプをサポート	このリリースでは、 AWS Config を使用して CloudFront ディストリビューションとストリーミングディストリビューションの設定変更を記録できます。 このリリースでは、 AWS Config を使用して、レートベースのルール、ルール、およびウェブ ACL の AWS WAF および AWS WAF リージョンリソースの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2017 年 11 月 15 日
AWS Config が AWS CodeBuild リソースタイプをサポート	このリリースでは、 AWS Config を使用して AWS CodeBuild プロジェクトの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2017 年 10 月 20 日

変更	説明	リリース日
AWS Config が Auto Scaling リソースと 1 つの新しいマネージドルールをサポート	このリリースでは、 AWS Config を使用して、グループ、起動設定、スケジュールされたアクション、スケーリングポリシーなどの Auto Scaling リソースの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。 このリリースでは、以下のマネージドルールもサポートしています。 • autoscaling-group-elb-healthcheck-required 詳細については、「AWS Config マネージドルール」を参照してください。	2017 年 9 月 18 日
AWS Config が AWS CodeBuild リソースタイプをサポート	このリリースでは、 AWS Config を使用して AWS CodeBuild プロジェクトの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2017 年 10 月 20 日

変更	説明	リリース日
AWS Config が Auto Scaling リソースと 1 つの新しいマネージドルールをサポート	このリリースでは、 AWS Config を使用して、グループ、起動設定、スケジュールされたアクション、スケーリングポリシーなどの Auto Scaling リソースの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。 このリリースでは、以下のマネージドルールもサポートしています。 • autoscaling-group-elb-healthcheck-required 詳細については、「AWS Config マネージドルール」を参照してください。	2017 年 9 月 18 日

変更	説明	リリース日
AWS Config が DynamoDB テーブルリソースタイプと 1 つの新しいマネージドルールをサポート	このリリースでは、 AWS Config を使用して DynamoDB テーブルの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。 このリリースでは、以下のマネージドルールをサポートしています。 • dynamodb-autoscaling-enabled 詳細については、「AWS Config マネージドルール」を参照してください。	2017 年 9 月 8 日
AWS Config が Amazon S3 の 2 つの新しいマネージドルールをサポート	このリリースでは 2 つの新しいマネージドルールをサポートしています。 • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited 詳細については、「AWS Config マネージドルール」を参照してください。	2017 年 8 月 14 日

変更	説明	リリース日
AWS Config コンソールの新しいページ	AWS Config コンソールで Dashboard を使用して、以下を確認できます。 • リソースの総数 • ルールの総数 • 非準拠リソースの数 • 非準拠ルールの数 詳細については、「AWS Config ダッシュボードの表示」を参照してください。	2017 年 7 月 17 日
新しい API オペレーション	GetDiscoveredResourceCounts オペレーションを使用して、 のリージョンで記録 AWS Config しているリソースタイプの数、各リソースタイプの数、およびリソースの総数を返すことができます AWS アカウント。	2017 年 7 月 17 日

変更	説明	リリース日
AWS Config が AWS CloudFormation スタックリソースタイプと 1 つの新しいマネージドルールをサポート	このリリースでは、 AWS Config を使用して AWS CloudFormation スタックの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。 このリリースでは、以下のマネージドルールをサポートしています。 • cloudformation-stack-notification-check 詳細については、「AWS Config マネージドルール」を参照してください。	2017 年 7 月 6 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、カナダ (中部) リージョンと南米 (サンパウロ) リージョンの AWS Config ルールのサポートが追加されました。 AWS Config および Config ルールをサポートするすべてのリージョンについては、のAWS リージョン 「」および「エンドポイント」を参照してくださいAWS 全般のリファレンス。	2017 年 7 月 5 日

変更	説明	リリース日
新しいコンテンツと更新されたコンテンツ	AWS Config ルールは AWS GovCloud (US) リージョンで使用できます。詳細については、「AWS GovCloud (US) ユーザーガイド」を参照してください。 がサポートするリージョンについては AWS Config、のAWS リージョン「」および「エンドポイント」を参照してくださいAWS 全般のリファレンス。	2017 年 6 月 8 日
AWS Config が Amazon CloudWatch アラームリソースタイプと 3 つの新しいマネージドルールをサポート	このリリースでは、 AWS Config を使用して Amazon CloudWatch アラームの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。 このリリースでは 3 つの新しいマネージドルールをサポートしています。 • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check 詳細については、「AWS Config マネージドルール」を参照してください。	2017 年 6 月 1 日

変更	説明	リリース日
新しいコンテンツと更新されたコンテンツ	このリリースでは、以下のマネージドルールで、アプリケーションバージョン番号の指定をサポートしています。 • ec2-managedinstance-applications-blacklisted • ec2-managedinstance-applications-required 詳細については、「AWS Config マネージドルール」を参照してください。	2017 年 6 月 1 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、アジアパシフィック (ムンバイ) リージョンの AWS Config ルールのサポートが追加されました。詳細については、「AWS 全般のリファレンス」の、「AWS リージョン とエンドポイント」を参照してください。	2017 年 4 月 27 日

変更	説明	リリース日
新しいコンテンツと更新されたコンテンツ	このリリースでは、アカウントに AWS Config マネージドルールを初めて追加するためのコンソール操作が更新されています。 初めて AWS Config ルールを設定するとき、または新しいリージョンでルールを設定するときは、マネージド AWS ルールを名前、説明、またはラベルで検索できます。[Select all] (すべて選択) ですべてのルールを選択し、[Clear all] (すべてクリア) ですべてのルールをクリアできます。 詳細については、「ルールの追加、表示、更新、削除 (コンソール)」を参照してください。	2017 年 4 月 5 日

変更	説明	リリース日
AWS Config が新しいマネージドルールをサポート	このリリースでは、以下の新しいマネージドルールをサポートしています。 • acm-certificate-expiration-check • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-inventory-blacklisted • ec2-volume-inuse-check • iam-user-group-membership-check • iam-user-no-policies-check • s3-bucket-ssl-requests-only 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2017 年 2 月 21 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、欧州 (ロンドン) リージョンの AWS Config ルールのサポートが追加されました。詳細については、「AWS 全般のリファレンス」の「AWS リージョン とエンドポイント」を参照してください。	2017 年 2 月 21 日

変更	説明	リリース日
新しいコンテンツと更新されたコンテンツ	このリリースでは、 AWS Config マネージドルールの AWS CloudFormation テンプレートが追加されました。このテンプレートを使用してアカウントのマネージドルールを作成できます。詳細については、「AWS CloudFormation テンプレートを使用した AWS Config マネージドルールの作成」を参照してください。	2017 年 2 月 16 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、`PutEvaluations` API の新しいテストモードのサポートを追加しています。 AWS Lambda 関数から AWS Configに評価結果が配信されることを確認するには、カスタムルールで `TestMode` パラメータを true に設定します。既存の評価は更新されません。また、AWS Configには評価結果が送信されません。 詳細については、「AWS Config API リファレンス」の [PutEvaluations] を参照してください。	2017 年 2 月 16 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、アジアパシフィック (ソウル) および米国西部 (北カリフォルニア) リージョンの AWS Config ルールのサポートが追加されました。詳細については、「AWS 全般のリファレンス」の「AWS リージョン とエンドポイント」を参照してください。	2016 年 12 月 21 日

変更	説明	リリース日
新しいコンテンツと更新されたコンテンツ	このリリースでは、欧州 (ロンドン) リージョン AWS Config での のサポートが追加されました。詳細については、「AWS 全般のリファレンス」の「AWS リージョン とエンドポイント」を参照してください。	2016 年 12 月 13 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、カナダ (中部) リージョン AWS Config での のサポートが追加されました。詳細については、「AWS 全般のリファレンス」の「AWS リージョン とエンドポイント」を参照してください。	2016 年 12 月 8 日

変更	説明	リリース日
AWS Config が Amazon Redshift リソースタイプと 2 つの新しいマネージドルールをサポート	このリリースでは、 AWS Config を使用して、Amazon Redshift クラスター、クラスターパラメータグループ、クラスターセキュリティグループ、クラスタースナップショット、クラスターサブネットグループ、イベントサブスクリプションの設定変更を記録できます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。 このリリースでは 2 つの新しいマネージドルールをサポートしています。 • redshift-cluster-configuration-check • redshift-cluster-maintenancesettings-check 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2016 年 7 月 12 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、新しいマネージドルールのサポートを追加しています。 • dynamodb-throughput-limit-check 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2016 年 7 月 12 日

変更	説明	リリース日
新しいコンテンツと更新されたコンテンツ	このリリースでは、アカウントのリージョンごとに最大 50 ルールの作成のサポートを追加しています。詳細については、「AWS 全般のリファレンス」の「AWS Config の制限」を参照してください。	2016 年 7 月 12 日
AWS Config が Amazon EC2 Systems Manager のマネージドインスタンスインベントリリソースタイプと 3 つの新しいマネージドルールをサポート	このリリースでは、 AWS Config を使用して、マネージドインスタンスインベントリをサポートするマネージドインスタンスのソフトウェア設定の変更を記録できます。 詳細については、「Recording Software Configuration for Managed Instances」を参照してください。 このリリースでは 3 つの新しいマネージドルールをサポートしています。 • ec2-managedinstance-inventory-blacklisted • ec2-managedinstance-applications-required • ec2-managedinstance-platform-check 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2016 年 12 月 1 日
新しいコンテンツと更新されたコンテンツ	AWS Config は、中国 (北京) リージョンで利用できます。	2016 年 10 月 24 日

変更	説明	リリース日
AWS Config が Amazon S3 バケットリソースと 2 つの新しいマネージドルールをサポート	このリリースでは、 AWS Config を使用して Amazon S3 バケットの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。 このリリースでは 2 つの新しいマネージドルールをサポートしています。 • s3-bucket-logging-enabled • s3-bucket-versioning-enabled 詳細については、「AWS Config マネージドルール」を参照してください。	2016 年 10 月 18 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、米国東部 (オハイオ) リージョンの AWS Config および AWS Config ルールのサポートが追加されました。詳細については、「AWS 全般のリファレンス」の「AWS リージョン とエンドポイント」を参照してください。	2016 年 10 月 17 日

変更	説明	リリース日
マネージドルールの新規追加および更新	この更新では、8 つの新しいマネージドルールのサポートを追加しています。 • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted 以下のルールには複数のパラメータ値を指定できます。 • desired-instance-tenancy • required-tags 詳細については、「AWS Config マネージドルールのリスト」を参照してください。	2016 年 10 月 4 日

変更	説明	リリース日
AWS Config コンソールの新規および更新されたコンテンツ	この更新により、 AWS Config タイムラインでの AWS CloudTrail API アクティビティの表示のサポートが追加されました。CloudTrail でアカウントのログを記録している場合、リソースの設定変更の作成、更新、および削除の API イベントを表示できます。詳細については、「を使用した AWS リソースのコンプライアンス履歴の表示 AWS Config」を参照してください。	2016 年 9 月 06 日
AWS Config が Elastic Load Balancing リソースタイプをサポート	このリリースでは、 AWS Config を使用して Elastic Load Balancing アプリケーションロードバランサーの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2016 年 8 月 31 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、アジアパシフィック (シンガポール) およびアジアパシフィック (シドニー) リージョンの AWS Config ルールのサポートが追加されました。詳細については、「AWS 全般のリファレンス」の「AWS リージョン とエンドポイント」を参照してください。	2016 年 8 月 18 日

変更	説明	リリース日
AWS Config ルールの新規および更新されたコンテンツ	この更新では、設定変更および指定間隔の両方でトリガーできるルールを作成するためのサポートを追加しています。詳細については、「AWS Config ルールのコンポーネント」を参照してください。 この更新では、ルールに対してリソースを手動で評価したり、評価結果を削除したりするためのサポートも追加されています。詳細については、「AWS Config ルールを使用したリソースの評価」を参照してください。 この更新では、カスタムルールを使用してその他のリソースタイプを評価するためのサポートも追加されています。	2016 年 7 月 25 日
AWS Config が Amazon RDS および AWS Certificate Manager (ACM) リソースタイプをサポート	このリリースでは、 AWS Config を使用して、Amazon Relational Database Service (Amazon RDS) DB インスタンス、DB セキュリティグループ、DB スナップショット、DB サブネットグループ、イベントサブスクリプションの設定変更を記録できます。 AWS Config を使用して、ACM が提供する証明書の設定変更を記録することもできます。 詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2016 年 7 月 21 日

変更	説明	リリース日
設定レコーダーの管理情報の更新	この更新では、設定レコーダーの名前変更および削除のステップを「設定レコーダーの使用」に追加しています。	2016 年 7 月 07 日
ロール作成の簡素化およびポリシーの更新	この更新により、 の IAM ロールの作成 AWS Config が簡素化されます。この機能強化は Config ルールをサポートするリージョンで使用できます。この機能強化をサポートするために、「コンソール AWS Config で をセットアップする」のステップ、「AWS Config 配信チャネルの Amazon S3 バケットのアクセス許可」のポリシー例、および「のアイデンティティベースのポリシーの例 AWS Config」のポリシー例が更新されています。	2016 年 3 月 31 日
Config ルールの関数例とイベント例	この更新では、更新されたサンプル関数が提供されます。	2016 年 3 月 29 日
AWS Config Rules GitHub リポジトリ	この更新では、AWS Config Rules GitHub リポジトリに関する情報が AWS Config ルールを使用したリソースの評価 に追加されています。このリポジトリは、 AWS Config ユーザーによって開発および提供されるカスタムルールのサンプル関数を提供します。	2016 年 3 月 1 日

変更	説明	リリース日
AWS Config ルール	このリリースでは、 AWS Config ルールが導入されました。ルールを使用すると、 AWS Config を使用して、 AWS リソースが目的の設定に準拠しているかどうかを評価できます。詳細については、「AWS Config ルールを使用したリソースの評価」を参照してください。	2015 年 12 月 18 日
AWS Config が IAM リソースタイプをサポート	このリリースでは、 AWS Config を使用して、IAM ユーザー、グループ、ロール、カスタマー管理ポリシーの設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2015 年 12 月 10 日
AWS Config が EC2 Dedicated Host をサポート	このリリースでは、 AWS Config を使用して EC2 Dedicated Hosts の設定変更を記録できます。詳細については、「でサポートされているリソースタイプ AWS Config」を参照してください。	2015 年 23 月 11 日

変更	説明	リリース日
アクセス許可情報の更新	この更新では、以下の AWS 管理ポリシーに関する情報が追加されました AWS Config。 • `AWS_ConfigRole` – リソースの設定の詳細を取得するためのアクセス許可を AWS Config に付与します。詳細については、「設定詳細を取得するための IAM ロールポリシー」を参照してください。 • `AWSConfigUserAccess` – AWS Config ユーザーへの読み取り専用アクセスを許可します。詳細については、「への読み取り専用アクセス AWS Config」を参照してください。	2015 年 10 月 19 日
AWS Config ルールのプレビュー	このリリースでは、 AWS Config ルールプレビューが導入されました。ルールを使用すると、 AWS Config を使用して、 AWS リソースが目的の設定に準拠しているかどうかを評価できます。詳細については、「AWS Config ルールを使用したリソースの評価」を参照してください。	2015 年 10 月 7 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、 AWS Config が検出したリソースを検索する機能が追加されました。詳細については、「によって検出されたリソースの検索 AWS Config」を参照してください。	2015 年 8 月 27 日

変更	説明	リリース日
新しいコンテンツと更新されたコンテンツ	このリリースでは、 AWS Config で記録するリソースタイプを選択する機能を追加しています。詳細については、「を使用した AWS リソースの記録 AWS Config」を参照してください。	2015 年 6 月 23 日
新しいコンテンツと更新されたコンテンツ	このリリースでは、アジアパシフィック (東京)、アジアパシフィック (シンガポール)、欧州 (フランクフルト)、南米 (サンパウロ)、米国西部 (北カリフォルニア) のリージョンのサポートが追加されています。詳細については、[AWS リージョン およびエンドポイント] を参照してください。	2015 年 4 月 6 日
新規ガイド	このリリースでは AWS Configを導入しています。	2014 年 11 月 12 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。